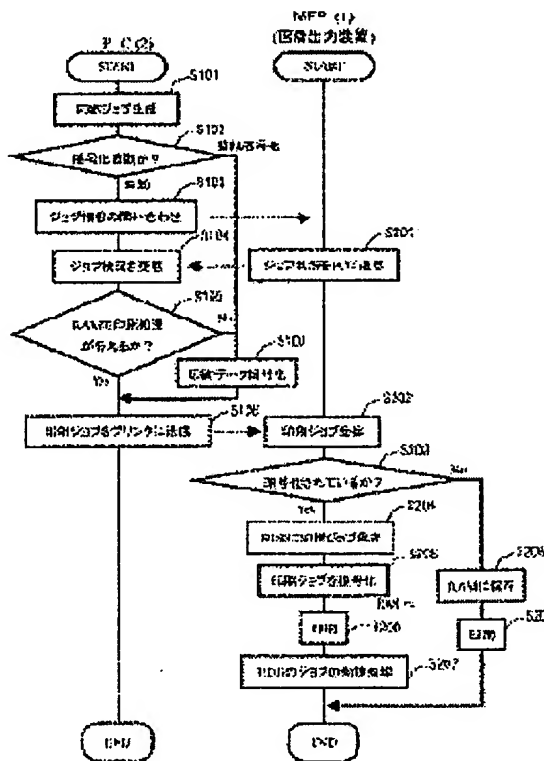


Related Reference NOT Cited in the Specification

Document Number or Title	Concise Explanation of Relevance for Non-English Language Information
Japanese Patent Laid-Open Publication No. 2004-336672 published on November 25, 2004	Disclosed is a technique encrypts received print data or deletes print data from a spool area after printing the data when a preset predictive condition for the occurrence of an anomalous condition is satisfied.

Priority number(s): JP20030155385 20030530: JP20030067464 20030313

COPYRIGHT: (C)2005,JPO&NCIPI



2006/08/17

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2004-336672

(P2004-336672A)

(43) 公開日 平成16年11月25日 (2004. 11. 25)

(51) Int. Cl. ⁷	F I	テーマコード (参考)
H04N 1/44	H04N 1/44	2C061
B41J 29/38	B41J 29/38	5B021
G06F 3/12	G06F 3/12	5C073
G09C 1/00	G09C 3/12	5C075
H04N 1/21	G09C 1/00 660D	5J104
審査請求 未請求 請求項の数 18 O L (全 21 頁) 最終頁に続く		

(21) 出願番号 特願2003-155385 (P2003-155385)
 (22) 出願日 平成15年5月30日 (2003. 5. 30)
 (31) 優先権主張番号 特願2003-67464 (P2003-67464)
 (32) 優先日 平成15年3月13日 (2003. 3. 13)
 (33) 優先権主張国 日本国 (JP)

(71) 出願人 000005049
 シャープ株式会社
 大阪府大阪市阿倍野区長池町22番22号
 (74) 代理人 100084135
 弁理士 本庄 武男
 (72) 発明者 河野 真一
 大阪府大阪市阿倍野区長池町22番22号
 シャープ株式会社内
 Fターム (参考) 2C061 AP01 AP03 AP04 AP07 HJ06
 HN23 HP00
 5B021 AA01 DD14 DD20 NN00
 5C073 AA00 AA06 BB01 BD03
 5C075 EE03 FF03 FF90
 5J104 AA12

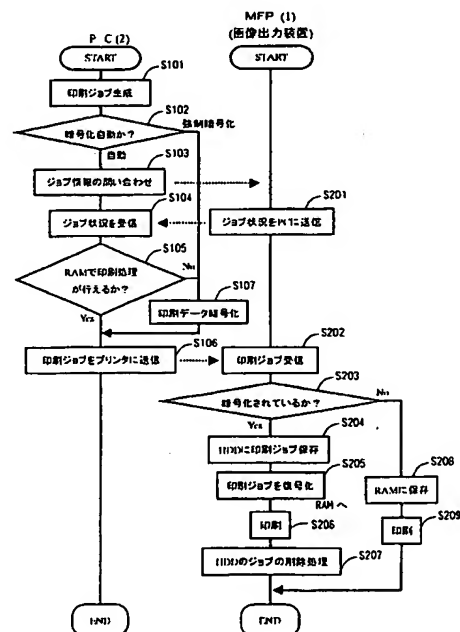
(54) 【発明の名称】 画像出力システム、画像データ送信プログラム及び画像出力装置

(57) 【要約】

【課題】 ネットワーク接続された画像出力装置に記憶される画像データのセキュリティを維持しながら処理時間を極力抑えること。

【解決手段】 画像出力装置 (MFP 1) から送信 (S201) される印刷ジョブの処理状況 (画像出力装置のRAMの使用状況、処理待ちの印刷ジョブのサイズや処理時間、画像処理の停止若しくはその兆候に関する情報) に基づいて、情報処理装置 (PC 2) において、印刷ジョブの暗号化を行うか否かを判別し (S105)、必要に応じて印刷ジョブを暗号化する (S107)。画像出力装置では、暗号化されている印刷ジョブを出力処理 (S206) 前に復号化する (S205)。出力処理が終了した印刷ジョブはHDD (不揮発性メモリ) から完全消去する (S207)。

【選択図】 図5



【特許請求の範囲】

【請求項 1】

情報処理装置から送信された画像データが画像出力装置により受信及び記憶手段への記憶がされ、該画像出力装置により前記画像データの出力がなされる画像出力システムにおいて、

前記画像出力装置における画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、

前記暗号化判別手段により暗号化を行うと判別された前記画像データを暗号化する暗号化手段と、

前記画像出力装置に設けられ暗号化されている前記画像データを出力処理前に復号化する復号化手段と、

前記画像出力装置に設けられ出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、

を具備してなることを特徴とする画像出力システム。

【請求項 2】

前記画像処理状況に関する情報が、前記記憶手段の一部を構成する揮発性メモリの使用状況に関する情報を含むものであり、

前記暗号化判別手段が、前記画像処理装置において前記記憶手段のうち前記揮発性メモリの範囲内の使用で処理できない前記画像データについて暗号化を行うと判別するものである請求項 1 に記載の画像出力システム。

【請求項 3】

前記画像処理状況に関する情報が、処理待ちの画像データの数量又はその処理時間に関する情報を含むものであり、

前記暗号化判別手段が、前記処理待ちの画像データの数量又はその処理時間が所定以上である場合に前記画像データの暗号化を行うと判別するものである請求項 1 又は 2 のいずれかに記載の画像出力システム。

【請求項 4】

前記画像処理状況に関する情報が、画像処理の停止及び／又は画像処理の停止の兆候に関する情報を含むものであり、

前記暗号化判別手段が、前記画像出力装置が画像処理の停止状態である場合又は画像処理の停止状態となる可能性が高い場合に前記画像データの暗号化を行うと判別するものである請求項 1 ～ 3 のいずれかに記載の画像出力システム。

【請求項 5】

前記画像処理の停止に関する情報が、記録紙の詰まり、記録紙切れ、現像剤切れ及び前記画像出力装置の故障のうちの 1 又は複数に関する情報である請求項 4 に記載の画像出力システム。

【請求項 6】

前記画像処理の停止の兆候に関する情報が、記録紙の残量及び／又は現像剤の残量に関する情報である請求項 4 に記載の画像出力システム。

【請求項 7】

前記画像データ消去手段が、暗号化されていない前記画像データはその出力処理の後直ちに前記記憶手段から消去するものである請求項 1 ～ 6 のいずれかに記載の画像出力システム。

【請求項 8】

前記画像データ消去手段が、暗号化されている前記画像データはその出力処理の後処理待ちの画像データがないときに前記記憶手段から消去するものである請求項 1 ～ 7 のいずれかに記載の画像出力システム。

【請求項 9】

前記画像出力装置が、前記画像処理状況に関する情報を前記情報処理装置に対して送信する画像処理情報送信手段を具備し、

10

20

30

40

50

前記情報処理装置が、前記画像出力装置から前記画像処理状況に関する情報を受信する画像処理情報受信手段と、前記暗号化判別手段と、前記暗号化手段とを具備してなる請求項 1 ～ 8 のいずれかに記載の画像出力システム。

【請求項 10】

前記画像出力装置が、前記暗号化判別手段と、前記暗号化手段とを具備してなる請求項 1 ～ 8 のいずれかに記載の画像出力システム。

【請求項 11】

前記画像出力装置が、前記暗号化判別手段と、該暗号化判別手段の判別結果情報を前記情報処理装置に対して送信する暗号化判別情報送信手段とを具備し、

前記情報処理装置が、前記画像出力装置から前記暗号化判別情報を受信する暗号化判別情報受信手段と、前記暗号化手段とを具備してなる請求項 1 ～ 8 のいずれかに記載の画像出力システム。

10

【請求項 12】

画像出力装置に対して画像出力に用いる画像データを送信する処理をコンピュータに実行させる画像データ送信プログラムにおいて、

前記画像出力装置から画像処理状況に関する情報を取得する画像処理情報取得処理と、

前記画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別処理と、

前記画像出力装置へ送信する前記画像データのうち前記暗号化判別処理によって暗号化を行うと判別されたものを暗号化する暗号化処理と、

20

をコンピュータに実行させることを特徴とする画像データ送信プログラム。

【請求項 13】

画像出力装置に対して画像出力に用いる画像データを送信する処理をコンピュータに実行させる画像データ送信プログラムにおいて、

前記画像データの暗号化を行うか否かに関する情報を前記画像出力装置から受信する暗号化情報受信処理と、

前記暗号化情報受信処理により暗号化を行う旨の情報を得た場合に前記画像出力装置に対して送信する画像データを暗号化する暗号化処理と、

をコンピュータに実行させることを特徴とする画像データ送信プログラム。

30

【請求項 14】

情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、

前記画像データの画像処理状況に関する情報を前記情報処理装置に対して送信する画像処理情報送信手段と、

暗号化されている前記画像データを出力処理前に復号化する復号化手段と、

出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、

を具備してなることを特徴とする画像出力装置。

【請求項 15】

情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、

40

前記画像データの画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、

前記暗号化判別手段により暗号化を行うと判別された前記画像データを暗号化する暗号化手段と、

暗号化されている前記画像データを出力処理前に復号化する復号化手段と、

出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、

を具備してなることを特徴とする画像出力装置。

【請求項 16】

情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、

50

前記画像データの画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、
前記暗号化判別手段の判別結果情報を前記情報処理装置に対して送信する暗号化判別情報送信手段と、
暗号化されている前記画像データを出力処理前に復号化する復号化手段と、
出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、
を具備してなることを特徴とする画像出力装置。

【請求項 17】

前記画像データ消去手段が、暗号化されていない前記画像データはその出力処理の後直ちに前記記憶手段から消去するものである請求項 14～16 のいずれかに記載の画像出力装置。

10

【請求項 18】

前記画像データ消去手段が、暗号化されている前記画像データはその出力処理の後処理待ちの画像データがないときに前記記憶手段から消去するものである請求項 14～17 のいずれかに記載の画像出力装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置から送信された画像データが画像出力装置により受信及び記憶され、該画像出力装置により前記画像データの出力がなされる画像出力システム及びその情報処理装置により実行される画像データ送信プログラム並びに画像出力装置に関するものである。

20

【0002】

【従来の技術】

パーソナルコンピュータ等の情報処理装置（以下、端末という）からネットワークを介してプリンタ等の画像出力装置にイメージ画像データやページ記述言語等で構成される印刷データ等の画像データを送信することにより画像出力を行う画像出力システムでは、画像出力装置が具備するメモリに一旦記憶（蓄積）されてから画像出力されることが一般的である。このような画像出力システムでは、画像出力装置のハードディスクドライブ（HDD）等のメモリが盗まれた場合や画像出力装置に対して不正アクセスがなされた場合等に、メモリに記憶された画像データのセキュリティ確保が問題となる。

30

従来、このような問題を解決するため、特許文献 1 には、HDD に記憶される印刷ジョブ（画像データの一例）を必ず暗号化することが示されている。

【0003】

【特許文献 1】

特開 2001-306273 号公報

【0004】

【発明が解決しようとする課題】

しかしながら、画像データを必ず暗号化することとすると、画像出力処理の前に必ず画像データの復号化処理を行う必要がある。このため、例えば、処理待ちの画像データがなく直ぐに出力処理ができるような画像処理状況であっても画像データの復号化が必要なため、出力処理がされるまでの時間が長くなるという問題点があった。

40

さらに、画像出力装置に記憶される画像データが暗号化されていても、その記憶状態が長時間に渡ると不正アクセスや盗難を受ける確率が高くなり、セキュリティが低下するという問題点もあった。例えば、処理待ちの画像データ（印刷ジョブ等）の数や処理量（出力部数等）が多い場合には、画像処理（印刷）が開始されるまでの処理待ち時間が長くなる。また、記録紙（用紙）の詰まり（ジャム）やトナー切れ（現像剤切れ）等により画像処理が停止状態となった場合には、ジャムの解除やトナーの補給等により画像処理の再開が可能となるまで画像処理が行えない。その結果、画像出力装置に画像データ（印刷ジョブ等）が長時間記憶される（滞留する）ことになり（備品の納期等によっては、復帰までに

50

数日間かかる場合も考えられる)、セキュリティの低下につながりやすい。

従って、本発明は上記事情に鑑みてなされたものであり、その目的とするところは、ネットワーク接続された画像出力装置に記憶される画像データのセキュリティを維持しながら処理時間を極力抑えることが可能な画像出力システム及びそれを構成する情報処理装置により実行される画像データ送信プログラム並びに画像出力装置を提供することにある。

【0005】

【課題を解決するための手段】

上記目的を達成するために本発明は、情報処理装置から送信された画像データが画像出力装置により受信及び記憶手段への記憶がされ、該画像出力装置により前記画像データの出力がなされる画像出力システムにおいて、前記画像出力装置における画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化を行うと判別された前記画像データを暗号化する暗号化手段と、前記画像出力装置に設けられ暗号化されている前記画像データを出力処理前に復号化する復号化手段と、出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、を具備してなることを特徴とする画像出力システムとして構成されるものである。

これにより、画像処理状況に応じて画像データの暗号化を行うか否かが決定されるので、例えば、新たな画像データを比較的短時間で出力処理できる画像処理状況にある場合等には、不正アクセスを受ける確率が低いので、暗号化を行わずに出力処理して処理時間を短縮するといった状況に応じた処理が可能となる。その結果、画像出力装置に記憶される画像データのセキュリティを維持しながら処理時間を極力抑えることが可能となる。

ここで、画像データの前記記憶手段からの消去形態としては、いわゆるFAT(File Allocation Tables)等の記憶手段内における画像データ自体へのアクセスを管理する情報(以下、データ管理情報という)のみを消去することも考えられるが、よりセキュリティ性を高めるためには、画像データ自体を所定の初期化データに書き換えることによって消去すること(以下、完全消去という)が望ましい。

【0006】

例えば、前記画像処理状況に関する情報が、前記記憶手段の一部を構成する揮発性メモリの使用状況に関する情報を含むものであり、前記暗号化判別手段が、前記画像処理装置において前記記憶手段のうち前記揮発性メモリの範囲内の使用で処理できない前記画像データについて暗号化を行うと判別するものが考えられる。

このような構成によれば、処理待ちの画像データが存在しない等により新たな画像データを前記揮発性メモリの範囲内の使用で処理できる場合には、画像が暗号化されずに(即ち、復号化の必要なく)出力処理が速くなる。一方、画像出力装置本体或いはその記憶手段が物理的に盗難された場合でも、揮発性メモリ内の暗号化されていないデータは、電源供給が途絶えるとともに消滅するので情報漏洩は生じない。また、一般的に、揮発性メモリの容量は比較的小さく、該メモリ内のデータは処理後に消去されるので、揮発性メモリに同じ画像データが蓄積されている時間は短く、この短時間の間に通信(ネットワーク)を介しての不正アクセスも生じにくい。これらの結果、画像データのセキュリティを維持しながら、復号化時間を省いて処理時間を極力抑えることが可能となる。

【0007】

また、前記画像処理状況に関する情報が、処理待ちの画像データの数量又はその処理時間に関する情報を含むものであり、前記暗号化判別手段が、前記処理待ちの画像データの数量又はその処理時間が所定以上である場合に前記画像データの暗号化を行うと判別するものも考えられる。

このような構成によっても、処理待ちの画像データの数量が少ない或いはその処理時間が所定未満である場合には、画像データが暗号化されずに(即ち、復号化の必要なく)出力処理が速くなる。同時に、この場合、画像データの処理が終了して消去されるまでの時間は比較的短く、この短時間の間に通信(ネットワーク)を介しての不正アクセスも生じにくい。これらの結果、画像データのセキュリティを維持しながら、復号化時間を省いて処

理時間を極力抑えることが可能となる。

【0008】

また、前記画像処理状況に関する情報が、画像処理の停止及び／又は画像処理の停止の兆候に関する情報を含むものであり、前記暗号化判別手段が、前記画像出力装置が画像処理の停止状態である場合又は画像処理の停止状態となる可能性が高い場合に前記画像データの暗号化を行うと判別するものが考えられる。

このような構成によれば、画像処理が停止状態でない或いは停止状態となる可能性が低い（停止の兆候がない）場合には、画像データが暗号化されずに（即ち、復号化の必要なく）出力処理が速くなる。同時に、この場合、新たな画像データの処理が開始されない或いは処理途中で中断状態となる可能性が低く、処理待ち或いは処理の中断の時間が長くなって記憶装置の盗難や不正アクセスを受ける可能性も低い。その結果、画像データのセキュリティを維持しながら、復号化時間を省いて処理時間を極力抑えることが可能となる。ここで、前記画像処理の停止に関する情報としては、例えば、記録紙の詰まり、記録紙切れ、現像剤切れ及び前記画像出力装置の故障のうちの1又は複数に関する情報等が考えられる。

10

また、前記画像処理の停止の兆候に関する情報としては、例えば、記録紙の残量及び／又は現像剤の残量に関する情報等が考えられる。

【0009】

また、前記画像データ消去手段としては、暗号化されていない前記画像データはその出力処理の後直ちに前記記憶手段から消去するものが考えられ、一方、暗号化されている前記画像データはその出力処理の後処理待ちの画像データがないときに前記記憶手段から消去するものが考えられる。

20

これにより、セキュリティ性の低い非暗号化データについては、最短の記憶時間で消去される。一方、比較的安全な暗号化されているデータについては、処理負荷がない（処理待ちの画像データがない）ときに消去処理されるので、出力処理の速度に影響を与えることがない。特に、画像データの前記完全消去を行う場合、該完全消去を行うのに時間を要するので、このような処理は出力速度への影響防止により効果的である。

【0010】

ここで、前記暗号化判別手段及び前記暗号化手段の両手段は、それぞれ前記情報処理装置側に設ける場合と前記画像出力装置側に設ける場合とが考えられる。

30

（前記両手段を情報処理装置に設ける場合）

例えば、前記画像出力装置が、前記画像処理状況に関する情報を前記情報処理装置に対して送信する画像処理情報送信手段を具備し、前記情報処理装置が、前記画像出力装置から前記画像処理状況に関する情報を受信する画像処理情報受信手段と、前記暗号化判別手段と、前記暗号化手段とを具備するものが考えられる。

（前記両手段を画像出力装置に設ける場合）

また、前記画像出力装置が、前記暗号化判別手段と、前記暗号化手段とを具備するものも考えられる。

（前記両手段を情報処理装置と画像出力装置とに分散して設ける場合）

さらに、前記画像出力装置が、前記暗号化判別手段と、該暗号化判別手段の判別結果情報を前記情報処理装置に対して送信する暗号化判別情報送信手段とを具備し、前記情報処理装置が、前記画像出力装置から前記暗号化判別情報を受信する暗号化判別情報受信手段と、前記暗号化手段とを具備するものも考えられる。

40

【0011】

また、本発明は、前記画像出力システムを構成する前記情報処理装置により実行される画像データ送信プログラムとして捉えたものであってもよい。これについても、前記暗号化判別手段及び前記暗号化手段の両手段を、それぞれ前記情報処理装置側に設ける場合と前記画像出力装置側に設ける場合とによって構成が異なる。

（前記両手段を情報処理装置に設ける場合）

例えば、画像出力装置に対して画像出力に用いる画像データを送信する処理をコンピュー

50

タに実行させる画像データ送信プログラムにおいて、前記画像出力装置から画像処理状況に関する情報を取得する画像処理情報取得処理と、前記画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別処理と、前記画像出力装置へ送信する前記画像データのうち前記暗号化判別処理によって暗号化を行うと判別されたものを暗号化する暗号化処理と、をコンピュータに実行させることを特徴とする画像データ送信プログラムが考えられる。

【0012】

(前記両手段を情報処理装置と画像出力装置とに分散して設ける場合)

或いは、画像出力装置に対して画像出力に用いる画像データを送信する処理をコンピュータに実行させる画像データ送信プログラムにおいて、前記画像データの暗号化を行うか否かに関する情報を前記画像出力装置から受信する暗号化情報受信処理と、前記暗号化情報受信処理により暗号化を行う旨の情報を得た場合に前記画像出力装置に対して送信する画像データを暗号化する暗号化処理と、をコンピュータに実行させることを特徴とする画像データ送信プログラムも考えられる。

10

【0013】

また、本発明は、前記画像出力システムを構成する前記画像出力装置として捉えたものであってもよい。これについても、前記暗号化判別手段及び前記暗号化手段の両手段を、それぞれ前記情報処理装置側に設ける場合と前記画像出力装置側に設ける場合とによって構成が異なる。

(前記両手段を情報処理装置に設ける場合)

例えば、情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、前記画像データの画像処理状況に関する情報を前記情報処理装置に対して送信する画像処理情報送信手段と、暗号化されている前記画像データを出力処理前に復号化する復号化手段と、出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、を具備してなることを特徴とする画像出力装置が考えられる。

20

【0014】

(前記両手段を画像出力装置に設ける場合)

或いは、情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、前記画像データの画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、前記暗号化判別手段により暗号化を行うと判別された前記画像データを暗号化する暗号化手段と、暗号化されている前記画像データを出力処理前に復号化する復号化手段と、出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、を具備してなることを特徴とする画像出力装置も考えられる。

30

【0015】

(前記両手段を情報処理装置と画像出力装置とに分散して設ける場合)

或いは、情報処理装置から送信された画像データを受信及び記憶手段への記憶を行い、該画像データの出力を行う画像出力装置において、前記画像データの画像処理状況に関する情報に基づいて前記画像データの暗号化を行うか否かを判別する暗号化判別手段と、前記暗号化判別手段の判別結果情報を前記情報処理装置に対して送信する暗号化判別情報送信手段と、暗号化されている前記画像データを出力処理前に復号化する復号化手段と、出力処理が終了した画像データを前記記憶手段から消去する画像データ消去手段と、を具備してなることを特徴とする画像出力装置も考えられる。

40

【0016】

以上のような画像出力装置においても、前記画像データ消去手段としては、暗号化されていない前記画像データはその出力処理の後直ちに前記記憶手段から消去するものが考えられ、一方、暗号化されている前記画像データはその出力処理の後処理待ちの画像データがないときに前記記憶手段から消去するものが考えられる。

【0017】

50

【発明の実施の形態】

以下添付図面を参照しながら、本発明の実施の形態及び実施例について説明し、本発明の理解に供する。尚、以下の実施の形態及び実施例は、本発明を具体化した一例であって、本発明の技術的範囲を限定する性格のものではない。

ここに、図1は本発明の実施の形態に係る画像出力システムXの概略構成を表す図、図2は本発明の実施の形態に係る画像出力システムXを構成するPC（パーソナルコンピュータ）及び画像出力装置の概略構成を表すブロック図、図3は本発明の実施の形態に係る画像出力システムXを構成する画像出力装置における印刷ジョブの処理状況に関するジョブ情報の構成例を表す図、図4は本発明の実施の形態に係る画像出力システムXにおける印刷ジョブの概略の伝送経路を模式的に表した図、図5は本発明の実施の形態に係る画像出力システムXにおける印刷ジョブの出力処理の手順を表すフローチャート、図6は本発明の実施の形態に係る画像出力システムXを構成するPCの画面例を表す図、図7は本発明の第1の実施例に係る画像出力システムにおける印刷ジョブの概略の伝送経路を模式的に表した図、図8は本発明の第1の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャート、図9は本発明の第1の実施例に係る画像出力システムにおける画像出力装置のハードディスクからの印刷ジョブの消去処理の手順を表すフローチャート、図10は本発明の第2の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャート、図11は本発明の第3の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャートである。

【0018】

まず、図1を用いて本発明の実施の形態に係る画像出力システムXの全体構成について説明する。

本画像出力システムXは、例えばIEEE802.3準拠等の所定のネットワーク3を介して、画像出力装置の一例である複合機能プリンタ1（MFP：Multi function Printer）と情報処理装置の一例である複数のPC2（パーソナルコンピュータ）とが通信可能に接続されて構成されている。

本画像出力システムXでは、印刷ジョブが前記PC2それぞれからネットワーク3を介して前記MFP1に対して送信され、これを受信した前記MFP1によりその印刷ジョブに対応する画像が記録紙に印刷（出力）される。

【0019】

図2は、前記PC2及び前記MFP1の概略構成を表すブロック図である。

図2に示すように、前記PC2は、各種演算を行うCPU21、該CPU21により実行されるプログラムが展開されるRAM22、前記CPU21により実行されるBIOS等のプログラムが記憶されるROM23、キーボードやマウス等の操作部24、液晶パネルやCRT等の表示部25、各種ドライバソフトやアプリケーションプログラム及び各種データが記憶されるハードディスクドライブ26（HDD）、前記ネットワーク3を介したデータ通信を行う通信部27等を具備する一般的なパーソナルコンピュータである。

前記HDD26には、印刷ジョブの元データとなる文書データや画像データ等を生成するためのワープロソフトや作画ソフト等の各種アプリケーションソフトP1、該アプリケーションソフトP1により作成されたデータを前記MFP1で解釈可能な印刷ジョブに変換し、該印刷ジョブを前記通信部27を介して前記MFP1に送信する処理を実行するためのプリンタドライバP2（画像データ送信プログラムの一例）等がインストールされている。印刷ジョブとしては、GDI（Graphics Device Interface）等のイメージデータや、PDL（Page Description Language：ページ記述言語）等で構成された16進数の命令体系データ等が考えられる。PDL等で構成された印刷ジョブについては、前記MFP1において印刷前にイメージデータに変換されてから印刷される。

ここで、前記プリンタドライバP2の特徴は、前記MFP1から印刷ジョブの処理状況（画像処理状況）に関する情報（以下、ジョブ情報という）を取得するジョブ情報取得処理と、該ジョブ情報取得処理により得られた情報に基づいて印刷ジョブの暗号化を行うか否

かを判別し、必要に応じて前記MFP1に送信する印刷ジョブを暗号化する暗号化処理とが実行可能に構成されていることである。その詳細については後述する。

【0020】

また、前記MFP1は、所定のプログラムが記憶されたROMを内蔵しそのプログラムを実行することにより当該MFP1の各種制御及び演算を行うCPU11、前記PC2から受信した印刷ジョブの処理状況の管理処理を実行するジョブ管理部12、印刷ジョブ（画像データ）を記憶する不揮発性メモリであるハードディスクドライブ13（HDD）、印刷ジョブをその出力処理の際に一時記憶する不揮発性メモリであるRAM14、原稿から画像を読み取るスキャナ19、該スキャナ19で読み取られた画像や前記PC2から受信した印刷ジョブについてインクジェット方式やレーザビーム方式等により記録紙への画像出力（画像形成）を行うプリントエンジン18、前記ネットワーク3を介して前記PC2と通信を行う通信部17、前記PC2から受信した印刷ジョブが暗号化されている場合に、その印刷ジョブを出力処理前に復号化する暗号復号部16、前記スキャナ19で読み取られた原稿画像データを電話回線を通じてFAX送信する機能や他のファクシミリ装置から電話回線を通じて受信した画像データを前記プリントエンジン18へ出力したり前記HDD13へ格納したりする機能を有するFAX機能部15等を具備している。前記スキャナ19により読み取られて画像出力する（即ち、原稿画像を複写する）画像データや前記FAX機能部15により受信される画像データも印刷ジョブの一つであり、その処理状況が前記ジョブ管理部12により管理される。

また、前記MFP1における前記通信部17と前記PC2における前記通信部27とは、前記ネットワーク3での通信途中で印刷ジョブが容易に傍受されないように、通信上の暗号化及びその復号化（HTTPS・IPsec・PPTP・L2TP等）を行う機能を有している。この通信上の暗号化・復号化は、前記プリンタドライバP2による暗号化及び前記暗号復号部16による復号化とは別に、必ず行われるものである。以下、「暗号化せずに印刷ジョブを送信」と表記した場合でも、この通信上の暗号化・復号化は行われるものとする。

【0021】

図3は、前記MFP1の前記ジョブ管理部12により管理される印刷ジョブの処理状況に関するジョブ情報JDの構成例を表すものである。

前記ジョブ管理部12は、印刷ジョブが前記PC2から受信或いは前記スキャナ19や前記FAX機能部15から入力されるごとに、その印刷ジョブの付加情報によるその印刷ジョブの送信者（送信元）の識別、その印刷ジョブが暗号化されているか否かの識別、その印刷ジョブがいずれの機能に対応するものであるのかの識別、その印刷ジョブの属性、その印刷ジョブのサイズ等の識別を行い、各印刷ジョブの到着順にジョブ番号D1を割り振って、各識別結果をユーザ名D2、暗号化情報D3、機能情報D5、属性情報D6、サイズ情報D7として所定の記憶手段に関連付けて記憶する。

ここで、前記機能情報D5は、前記PC2から受信した印刷ジョブを出力するプリンタ機能、前記スキャナ19で読み取られた画像データ（印刷ジョブ）を出力するコピー機能、前記FAX機能部15にて受信された画像データ（印刷ジョブ）を出力するFax機能等の識別情報である。

また、前記属性情報D6は、その印刷ジョブが、出力処理の待ち行列に加えるべき通常の印刷ジョブ（「待ち」）であるのか、特定の利用者宛ての親展ジョブでありその利用者からパスワード等の指定により出力命令があるまで出力せずに（出力処理の待ち行列に加えずに）前記HDD13に格納しておくべき印刷ジョブであるのかの識別情報である。

さらに、前記ジョブ管理部12は、前記HDD13及び前記RAM14内のデータの格納状況や他の機器の動作状況を常時監視し、各印刷ジョブがどのような状態であるかをチェックしてその状態D4も前記ジョブ番号D1に関連付けて記憶する。例えば、その印刷ジョブが前記HDD13に保存されて処理待ちの状態にあるのか（「HDD保存」）、前記RAM14に転送されて前記プリントエンジン18により出力中であるのか（「印字中」）、前記通信部17等により受信中であるのか（「受信中」）等の状態D4が管理される

前記ジョブ管理部 12 により、これらの情報 D 1 ~ D 7 を含むジョブ情報 J D が常に最新の状態に維持されるよう管理される。そして、出力処理が完了して前記 R A M 1 4 及び前記 H D D 1 3 から消去された印刷ジョブは、前記ジョブ情報 J D から消去され、その消去に応じて前記ジョブ番号 D 1 が新たに割り振られる。ここで、前記印刷ジョブの消去は、前記完全消去により消去される。

【0022】

本画像出力システム X では、前記 P C 2 の前記プリンタドライバ P 2 の処理により、前記ジョブ情報 J D の前記状態 D 4 が前記 M F P 1 から取得され、取得された前記状態 D 4 に基づいて前記 M F P 1 の前記 R A M 1 4 の範囲内のメモリ使用で（即ち、前記 H D D 1 3 を使用せずに）画像データの出力処理を行うことができると判断される場合に、印刷ジョブを暗号化しないと判別される。これに対し、前記 M F P 1 の前記 R A M 1 4 の範囲内のメモリ使用で（即ち、前記 H D D 1 3 を使用しなければ）画像データの出力処理を行うことができないと判断される場合には、印刷ジョブを暗号化すると判別される。

本画像出力システム X では、前記 R A M 1 4 の範囲内のメモリ使用で出力処理を行えるか否かの判断は、前記 P C 2 の前記プリンタドライバ P 2 の処理により、以下の基準で行われる。

即ち、前記ジョブ情報 J D における前記状態 D 4（前記揮発性メモリの使用状況に関する情報の一例）に、「印字中」である印刷ジョブが存在しない場合には、前記 M F P 1 の前記 R A M 1 4（揮発性メモリ）が未使用であり、該 R A M 1 4 の範囲内のメモリ使用で処理できると判断される。これに対し、前記状態 D 4 に「印字中」である印刷ジョブが存在する場合には、前記 M F P 1 の前記 R A M 1 4 が使用中であり、該 R A M 1 4 の範囲内のメモリ使用で処理できないと判断される。

【0023】

ここで、前記 R A M 1 4 の範囲内のメモリ使用で出力処理を行えるか否かの判断は、上記以外の基準で行うものであってもよい。

例えば、前記ジョブ情報 J D に、前記 R A M 1 4 の空き容量の情報（前記揮発性メモリの使用状況に関する情報の一例）を含め、前記 P C 2 側において、前記 R A M 1 4 の空き容量が、印刷ジョブのデータサイズに比べて十分である場合に、前記 R A M 1 4 の範囲内のメモリ使用で出力処理を行えると判別すること等が考えられる。

【0024】

図 4（a）は、暗号化されていない印刷ジョブの概略の伝送経路を矢印によって模式的に表したものである。図 4 において、網掛け枠で示す印刷ジョブが暗号化された印刷ジョブを表し、白抜き枠で示す印刷ジョブが暗号化されていない印刷ジョブを表す。

図 4（a）に示すように、暗号化されていない印刷ジョブが前記 P C 2 側から送信されると、その印刷ジョブは前記 M F P 1 側で前記 H D D 1 3 に格納されずに直接前記 R A M 1 4 に一時記憶されて前記プリントエンジン 18 による出力処理が行われる。

一方、図 4（b）は、暗号化されている印刷ジョブの概略の伝送経路を矢印によって模式的に表したものである。図 4（b）に示すように、暗号化されている印刷ジョブが前記 P C 2 側から送信されると、その印刷ジョブは前記 M F P 1 側で前記 H D D 1 3 に一旦格納され（その際、その印刷ジョブは出力処理の待ち行列に加えられる）、処理の順番がきた時点で前記暗号復号部 16 によって復号化されるとともに、前記 R A M 1 4 に一時記憶されて前記プリントエンジン 18 による出力処理が行われる。

【0025】

次に、図 5 に示すフローチャートを用いて、印刷ジョブの出力処理の手順について説明する。以下、S 101、S 102、…は、処理手順（ステップ）の番号を表す。図 5 において、前記 P C 2 側の処理は、前記プリンタドライバ P 2 の処理（実行するのは前記 C P U 2 1）によって制御され、前記 M F P 1 側の処理は、前記 C P U 1 1 によって制御される。

まず、前記 P C 2 側において、ワープロ等のアプリケーションソフト P 1 が起動され、前

10

20

30

40

50

記操作部 24 から作成されたデータの印刷開始操作がなされると、前記プリンタドライバ P2 によって印刷ジョブが生成（作成）される（S101）。

次に、前記 PC2 の表示部 25 によって図 6 に示すような入力要求画面が表示され、印刷ジョブの暗号化を自動モード M1（「自動」）で行うか強制暗号化モード M2（「必ず暗号化」）で行うかの選択入力処理がなされる（S102）。このとき、前記ジョブ情報 JD における前記属性情報 D6 の元になる親展情報 D6' の入力処理もなされる。この入力処理では、印刷ジョブを親展ジョブとするか否かの選択及び親展ジョブとする場合のパスワードの入力が行われる。この親展情報 D6' は、印刷ジョブの付加情報として前記 MFP1 に送信される。

【0026】

S102 において、前記自動モード M1 が選択された場合には、前記通信部 27 から前記 MFP1 に対して前記ジョブ情報 JD の要求が送信される（S103（ジョブ情報の問い合わせ））。これに対し、前記 MFP1 側では、その要求に応じて前記ジョブ管理部 12 から前記通信部 17 を通じて最新の前記ジョブ情報 JD が返信される（S201（ジョブ状況を PC に送信））。

このように返信された前記ジョブ情報 JD は、前記 PC2 側の前記通信部 27 で受信され（S104（ジョブ状況を受信））、印刷ジョブの出力処理（印刷処理）が前記 MFP1 側の前記 RAM14 の範囲内のメモリ使用で実行できるか否かが判別される（S105）。この判別（判断）は、前述したように、前記ジョブ情報 JD における前記状態 D4 に「印字中」であるものがあるか否かを基準にして行われる。

S105 において、前記 RAM14 の範囲内のメモリ使用で実行できないと判別された場合、又は S102 において、前記強制暗号化モード M2 が選択された場合は、前記プリンタドライバ P2 によって印刷ジョブが暗号化（S107）された後、該暗号化後の印刷ジョブが前記通信部 27 を通じて前記 MFP1 に対して送信され（S106）、前記 PC2 側の処理が終了する。

また、S105 において、前記 RAM14 の範囲内のメモリ使用で実行できると判別された場合は、印刷ジョブは暗号化されずにそのまま前記通信部 27 を通じて前記 MFP1 に対して送信され（S106）、前記 PC2 側の処理が終了する。

【0027】

一方、前記 MFP1 側においては、前記 PC2 からの印刷ジョブが前記通信部 17 を通じて受信され（S202）、その印刷ジョブが暗号化されているか否かが判別される（S203）。

ここで、受信した印刷ジョブが暗号化されていない場合には、その印刷ジョブは前記 RAM14 に直接格納（保存）され（S208）、前記プリントエンジン 18 によって印刷処理（出力処理）（S209）がなされた後、前記 MFP1 側の処理が終了する。このとき、前記 RAM14 内の印刷ジョブは、出力処理の終了とともに前記 RAM14 内から消去される。ここで、前記 RAM14（揮発性メモリ）からの印刷ジョブの消去は、前記完全消去ではなく FAT 等の前記データ管理情報のみを消去する。これは、前記 MFP1 自体或いは前記 RAM14 が物理的に盗難された場合でも、前記 RAM14 内のデータは、電源供給が途絶えるとともに消滅するので情報漏洩は生じないからであり、その方が消去時間を短縮できるからである。もちろん、より機密性を高める場合には前記完全消去を行ってもよい。

また、S203 において、受信した印刷ジョブが暗号化されていると判別された場合には、その印刷ジョブは前記 HDD13 に一旦格納（保存）され、出力処理の待ち行列に加えられる（S204、前記ジョブ管理部 12 により前記ジョブ情報 JD の前記状態 D3 が「HDD 保存」と設定される）。

そして、前記 HDD13 に格納された印刷ジョブは、その処理の順番がきた時点で前記暗号復号部 16 によって復号化される（暗号化が解除される）とともに、前記 RAM14 に一時記憶され（S205）、さらに前記プリントエンジン 18 による出力（印刷）処理が行われる（S206）。

10

20

30

40

50

そして、出力処理が終了した印刷ジョブは、前記HDD13から消去（前記完全消去）（S207）された後、前記MFP1側の処理が終了する。もちろん、前記HDD13に格納されている印刷ジョブは暗号化されているので、前記完全消去をせずに、FAT等の前記データ管理情報のみを消去するようにしてもよい。そうすれば、印刷ジョブの前記HDD13から前記完全消去を行うよりも処理時間が短縮される。

【0028】

以上示したように、本画像出力システムXによれば、前記MFP1（画像出力装置）側の前記RAM14の使用状況に応じて、印刷ジョブの暗号化／非暗号化が切り替えられるため、前記RAM14の範囲で出力処理を行うことができる場合には、復号化処理及び暗号化された元の印刷ジョブの消去処理を行う必要がなく、処理時間を短く抑えることができる。

10

しかも、前記RAM14に一時記憶される時間はごく短時間であるため、不正アクセスによるデータ漏洩も発生しにくい。さらに、不揮発性メモリである前記RAM14は、電源供給が途絶えると記憶内容が残らないため、メモリの盗難によるデータ漏洩も発生しない。

【0029】

【実施例】

（第1の実施例）

前記画像出力システムXでは、印刷ジョブを暗号化するか否かを、前記MFP1の前記RAM14の範囲内のメモリ使用で出力処理を行えるか否かによって判別するものであったが、これに限るものでなく他の基準により判別するものも考えられる。ここでは、印刷ジョブを暗号化するか否かを、処理待ちの印刷ジョブのデータサイズ（量）が所定サイズ以上であるか否かによって判別する第1の実施例について説明する。

20

この第1の実施例においても、前記実施の形態と同様に、前記PC2の前記プリンタドライバP2の処理により、前記ジョブ情報JDの前記状態D4が前記MFP1から取得され、取得された前記状態D4に基づいて印刷ジョブを暗号化するか否かが判別されるものとする。

図7（a）は、前記MFP1における処理待ちの印刷ジョブの合計サイズが、所定の暗号化なし許容サイズW未満であるため、暗号化されていない印刷ジョブが伝送される場合の概略伝送経路を矢印によって模式的に表したものである。図7において、網掛け枠で示す印刷ジョブが暗号化された印刷ジョブを表し、白抜き枠で示す印刷ジョブが暗号化されていない印刷ジョブを表す。

30

図7（a）に示すように、前記PC2側から送信された印刷ジョブが暗号化されていないものであっても、その印刷ジョブは前記MFP1側で前記HDD13に格納され（その際、その印刷ジョブは出力処理の待ち行列に加えられる）、処理の順番がきた時点で、前記RAM14に一時記憶されて前記プリントエンジン18による出力処理が行われる。

一方、図7（b）は、前記MFP1における処理待ちの印刷ジョブの合計サイズが、所定の暗号化なし許容サイズW以上であるため、暗号化された印刷ジョブが伝送される場合の概略伝送経路を矢印によって模式的に表したものである。図7（b）に示すように、暗号化されている印刷ジョブが前記PC2側から送信されると、その印刷ジョブは前記MFP1側で前記HDD13に一旦格納され（その際、その印刷ジョブは出力処理の待ち行列に加えられる）、処理の順番がきた時点で前記暗号復号部16によって復号化されるとともに、前記RAM14に一時記憶されて前記プリントエンジン18による出力処理が行われる。

40

【0030】

ここで、「印刷ジョブのサイズ」としては、印刷ジョブがイメージデータ（ビットデータ）を主体に構成されている場合には印刷ジョブ自体のデータサイズ（byte等）を用いることが考えられるが、印刷ジョブがページ記述言語（PDL：page description language）により構成される場合には、その印刷ジョブの内容から出力画像のデータサイズを推定演算した実質的な値（サイズ）を用いる。例えば、印刷ジ

50

ジョブに設定される印刷部数の指定コマンドを参照し、その印刷部数に応じてデータサイズの値を加算（掛け算）する等である。また、出力画像のデータサイズが同じでも、その画像内容によっては画像形成に要する時間が異なる場合もある。このため、PDLにより構成される印刷ジョブに設定されるコマンドごとに処理時間を予め登録（記憶）しておき、印刷ジョブの内容からその処理時間を推定演算した時間換算値を印刷ジョブのサイズに置き換えて用いることも考えられる。以下、「印刷ジョブの（合計）サイズ」には、上記のように推定演算した値も含まれるものとする。

【0031】

次に、図8に示すフローチャートを用いて、第1の実施例における印刷ジョブの出力処理の手順について説明する。図8において、前記PC2側の処理は、前記プリンタドライバP2の処理（実行するのは前記CPU21）によって制御され、前記MFP1側の処理は、前記CPU11によって制御される。

10

図8における前記PC2側のS301～S304の処理、及びこれに対応する前記MFP1側のS401の処理は、図5で示した前記画像出力システムXにおけるS101～S104及びS201の処理と同じであるので、ここでは説明を省略する。

前記PC2側において、前記通信部27により前記MFP1側から前記ジョブ情報JDが受信（S304）されると、該ジョブ情報JDに基づいて前記MFP1における処理待ちの印刷ジョブの合計サイズが、前記暗号化なし許容サイズW以上であるか否かが判別される（S305）。ここで、処理待ちの印刷ジョブの合計サイズは、前記ジョブ情報JDにおける前記属性情報D6が「待ち」である印刷ジョブについての前記サイズ情報D7を合計することによって求められる。

20

S105において、処理待ちの印刷ジョブの合計サイズが前記暗号化なし許容サイズW以上であると判別された場合、又はS302において、前記強制暗号化モードM2が選択された場合は、前記プリンタドライバP2によって印刷ジョブが暗号化（S307）された後、該暗号化後の印刷ジョブが前記通信部27を通じて前記MFP1に対して送信され（S306）、前記PC2側の処理が終了する。

また、S305において、処理待ちの印刷ジョブの合計サイズが前記暗号化なし許容サイズW未満であると判別された場合には、印刷ジョブは暗号化されずにそのまま前記通信部27を通じて前記MFP1に対して送信され（S306）、前記PC2側の処理が終了する。

30

【0032】

一方、前記MFP1側においては、前記PC2からの印刷ジョブが前記通信部17を通じて受信され（S402）、その印刷ジョブが処理待ちする必要があるか否か（即ち、前記属性情報D6が「待ち」の印刷ジョブが既に存在するか否か）が判別される（S403）。

ここで、受信した印刷ジョブが処理待ちの必要がないと判別された場合には、その印刷ジョブは前記RAM14に直接格納（保存）され（S408）、前記プリントエンジン18によって印刷処理（出力処理）（S409）がなされた後、前記MFP1側の処理が終了する。このとき、前記RAM14内の印刷ジョブは、出力処理の終了とともに前記RAM14内から消去される。

40

また、S403において、受信した印刷ジョブが処理待ちの必要があると判別された場合には、その印刷ジョブは前記HDD13に一旦格納（保存）され、出力処理の待ち行列に加えられる（S404、前記ジョブ管理部12により前記ジョブ情報JDの前記状態D3が「HDD保存」と設定される）。

そして、前記HDD13に格納された印刷ジョブは、その処理の順番がきた時点で暗号化されているか否かがチェックされ、暗号化されていれば前記暗号復号部16によって復号化された後、暗号化されていなければそのまま前記RAM14に一時記憶され（S405）、さらに前記プリントエンジン18による出力（印刷）処理が行われる（S406）。そして、出力処理が終了した印刷ジョブは、後述する前記HDD13からの印刷ジョブの消去処理により消去（S407）された後、前記MFP1側の処理が終了する。

50

【0033】

図9は、前記HDD13からの印刷ジョブの消去処理の手順を表すフローチャートである。この処理は、前記MFP1の前記CPU11によって制御される。

この消去処理では、出力処理が済んだ前記HDD13内の印刷ジョブが暗号化されたものであるか否かが判別され(S501)、暗号化されていなければ直ちにその印刷ジョブが前記HDD13から前記完全消去がなされ(S502)、暗号化されている場合は、処理待ちの印刷ジョブがなくなるまで待つて(もちろん、既に処理待ちの印刷ジョブがない場合は直ちに)前記HDD13から前記完全消去がなされる。ここで、印刷ジョブが暗号化されている場合は、FAT等の前記データ管理情報のみを消去するようにしてもよい。

【0034】

以上示したように、本第1の実施例に係る画像出力システムによれば、前記MFP1(画像出力装置)側の出力処理待ちの印刷ジョブのサイズ(量)に応じて、印刷ジョブの暗号化/非暗号化が切り替えられるため、処理待ちの印刷ジョブのサイズが小さい場合には、復号化処理を行う必要がなく、処理時間を短く抑えることができる。

しかも、処理待ちの印刷ジョブのサイズが小さければ、新たに追加された印刷ジョブの出力完了及びその直後の消去までの時間は比較的短時間であるため、不正アクセスによるデータ漏洩も発生しにくい。

一方、処理待ちの印刷ジョブのサイズ(合計サイズ)が大きい場合には、印刷ジョブが暗号化されるため、処理待ち中に不正アクセス等によってデータ漏洩すること(セキュリティの低下)を防止できる。

また、処理待ちの印刷ジョブのサイズが大きい(処理時間が長い)ということは、先行の印刷ジョブの処理中にトナー切れや記録紙切れ、ジャム等の画像処理の停止につながるトラブルが発生する確率も高くなる。従って、このようなトラブルの発生によって印刷ジョブ(画像データ)の滞留時間がより長くなり、不正アクセスや盗難を受ける可能性がより高くなるが、この場合には印刷ジョブが暗号化されているので、セキュリティの低下が最小限に抑えられる。

さらに、比較的安全な暗号化された印刷ジョブについては、処理待ちの印刷ジョブがなくなってから削除されるため、印刷ジョブの前記HDD13からの消去時間が他の印刷ジョブの処理時間に影響を与えない。

【0035】

(第2の実施例)

前記実施の形態及び前記第1の実施例は、いずれも印刷ジョブを暗号化するか否かの判別及び印刷ジョブの暗号化を前記PC2側(情報処理装置側)で行うものであったが、これに限るものでなく、前記MFP1側(画像出力装置側)で行うものであってもよい。

図10は、印刷ジョブを暗号化するか否かの判別及び印刷ジョブの暗号化を前記MFP1で行う第2の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャートである。

まず、前記PC2側において、ワープロ等のアプリケーションソフトP1が起動され、前記操作部24から作成されたデータの印刷開始操作がなされると、前記プリンタドライバP2によって印刷ジョブが生成(作成)される(S601)。

次に、前記PC2の表示部25によって暗号化を前記自動モードM1で行うか前記強制暗号化モードM2で行うかの選択入力処理及び前記親展情報D6'の入力処理がなされる(S602(図6参照))。ここで入力される前記親展情報D6'は、印刷ジョブの付加情報として前記MFP1に送信される。

S602において、前記自動モードM1が選択された場合には印刷ジョブに前記自動モードM1である旨の識別情報が付加され(S604)、前記強制暗号化モードM2が選択された場合には印刷ジョブに前記強制暗号化モードM2である旨の識別情報が付加される(S603)。

そして、前記識別情報とともに印刷ジョブがそのまま暗号化されずに前記通信部27を通じて前記MFP1側へ送信され(S605)、前記PC2側の処理が終了する。

10

20

30

40

50

【0036】

一方、前記MFP1側においては、前記PC2からの印刷ジョブが前記通信部17を通じて受信され(S701)、その印刷ジョブの暗号化の要否が判別される(S702)。ここでは、印刷ジョブが前記強制暗号化モードM2である旨の情報が付加されている場合には、前記ジョブ情報JDの内容にかかわらず、暗号化が必要であると判別される。

また、前記自動モードM1である旨の情報が付加されている場合には、前記ジョブ情報JDに基づいて前述した図5におけるS105の判別基準に従って、印刷ジョブを暗号化するか否か(要否)が判別される。

S702において、印刷ジョブの暗号化が不要と判別された場合には、その印刷ジョブは前記RAM14に直接格納(保存)され(S708)、前記プリントエンジン18によって印刷処理(出力処理)(S709)がなされた後、前記MFP1側の処理が終了する。このとき、前記RAM14内の印刷ジョブは、出力処理の終了とともに前記RAM14内から消去される。

10

また、S702において、受信した印刷ジョブの暗号化が必要と判別された場合には、前記暗号復号部16によってその印刷ジョブが暗号化され(S703)、暗号化された印刷ジョブが前記HDD13に格納(保存)される(S704)。このとき、その印刷ジョブは、出力処理の待ち行列に加えられる(前記ジョブ管理部12により前記ジョブ情報JDの前記状態D3が「HDD保存」と設定される)。なお、前記暗号復号部16は、暗号化機能に加え、復号化機能も有するものとする。

そして、前記HDD13に格納された印刷ジョブは、その処理の順番がきた時点で前記暗号復号部16によって復号化される(暗号化が解除される)とともに、前記RAM14に一時記憶され(S705)、さらに前記プリントエンジン18による出力(印刷)処理が行われる(S706)。

20

次に、出力処理が終了した印刷ジョブは、前記HDD13から前記完全消去(S707)がなされた後、前記MFP1側の処理が終了する。もちろん、前記HDD13に格納されている印刷ジョブは暗号化されているので、前記完全消去をせずにFAT等の前記データ管理情報のみを消去するようにしてもよい。

この第2の実施例の構成によれば、MFP1側で暗号化が行われるので、前記PC2から送信される印刷ジョブだけでなく、コピーのジョブやFAXのジョブ等についても前記PC2側からの印刷ジョブと同様に暗号化を行うことができる点でよりセキュリティ上効果的である。

30

【0037】

また、前記MFP1側で暗号化を行うか否かの判別までを行い、その判別結果を前記PC2に対して送信し、これを受信した前記PC2側において、受信した前記判別結果に従って、必要な場合にのみ印刷ジョブの暗号化を行うよう構成してもよい。

例えば、図5のS103を、前記PC2から前記MFP1に対して暗号化を行うか否かに関する暗号化判別情報を要求する処理に置き換える。この要求を受けた前記MFP1側では、暗号化を行うか否かの判別処理(例えば、図10のS702の処理)の後、図5のS201の代わりに前記MFP1からその判別結果を前記暗号化識別情報として前記PC2へ返信するよう構成する。

40

さらに、前記PC2側のS105の判別処理を、前記暗号化識別情報に従って暗号化を行う(S107)か否かが切り替わるよう構成する。本発明は、このような構成によって具現することも考えられる。

【0038】

(第3の実施例)

前記実施の形態及び前記第1の実施例は、印刷ジョブを暗号化するか否かを、前記MFP1の前記RAM14の範囲内のメモリ使用で出力処理を行えるか否かによって判別する、或いは処理待ちの印刷ジョブのデータサイズ(量)が所定サイズ以上であるか否かによって判別するものであったが、これに限るものでなく他の基準により判別するものも考えられる。ここでは、印刷ジョブを暗号化するか否かを、画像処理の停止やその兆候に関する

50

情報を基準に判別する第3の実施例に係る画像出力システムについて説明する。

図11は、本発明の第3の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャートである。

図11に示すS801～S806は、前述した図5のS101～S106に

図11における前記PC2側のS801～S806の処理、及びこれに対応する前記MFP1側のS901～S909の処理は、図5で示した前記画像出力システムXにおけるS101～S106及びS201～S209の処理に対応する。ここで、図11に示す処理と図5に示した処理とで異なる点は、S901及びS804で送受信される情報が、前記ジョブ情報JDではなく、前記MFP1における画像処理の停止やその兆候に関する情報（以下、装置情報という）である点、及び前記PC2側におけるS805の処理が、前記装置情報に基づいて印刷ジョブを暗号化するか否かを判別する処理である点であり、その他の処理は図5に示した処理と同じである。

10

【0039】

前記装置情報には、前記MFP1におけるジャム（記録紙の詰まり）、記録紙切れ（用紙切れ）、トナー切れ（現像剤切れ）、前記MFP1の故障に関する情報（前記画像処理の停止に関する情報の一例）と、記録紙の残量（残枚数）、トナー（現像剤）の残量に関する情報（画像処理の停止の兆候に関する情報の一例）とが含まれている。

そして、前記PC2側のS805において、ジャムが発生している場合、記録紙切れが発生している場合、トナー切れが発生している場合及び前記MFP1に故障が発生している場合、さらに、記録紙の残量（残枚数）が所定枚数未満である場合又はトナー残量が所定量未満である場合には、印刷ジョブは前記プリンタドライバP2によって暗号化（S807）された後、それ以外の場合には印刷ジョブは暗号化されずに前記通信部27を通じて前記MFP1に対して送信され（S806）、前記PC2側の処理が終了する。

20

これにより、ジャムの解除や記録紙、トナーの補給等により画像処理の再開が可能となるまで画像処理が行えない。

これにより、ジャムやトナー切れ等によって画像処理が停止状態でない場合や、記録紙残量やトナー残量が少ないために処理が途中で停止状態となる可能性が低い（停止の兆候がない）場合には、印刷ジョブ（画像データ）が暗号化されないため（即ち、復号化の必要がないため）画像の出力処理が速くなる。同時に、印刷ジョブの処理が開始されない或いは処理途中で中断状態となる可能性が低く、処理待ち或いは処理の中断の時間が長くなって前記画像メモリ13の盗難やネットワークを通じた不正アクセスを受ける可能性も低い。その結果、印刷ジョブのセキュリティを維持しながら、復号化時間を省いて処理時間を極力抑えることが可能となる。

30

また、このように印刷ジョブを暗号化するか否かを、画像処理の停止やその兆候に関する情報を基準に判別する場合にも、図10に示したものと同様の手順により、印刷ジョブを暗号化するか否かの判別及び印刷ジョブの暗号化を、前記MFP1で行うように構成することが考えられる。この場合、図10のS702の判別処理において、図11のS805と同様の判別処理を実行すればよい。

【0040】

【発明の効果】

40

以上説明したように、本発明によれば、画像処理状況に応じて画像データの暗号化を行うか否かが決定されるので、画像出力装置に記憶される画像データのセキュリティを維持しながら処理時間を極力抑えることが可能となる。

【図面の簡単な説明】

【図1】本発明の実施の形態に係る画像出力システムXの概略構成を表す図。

【図2】本発明の実施の形態に係る画像出力システムXを構成するPC（パーソナルコンピュータ）及び画像出力装置の概略構成を表すブロック図。

【図3】は本発明の実施の形態に係る画像出力システムXを構成する画像出力装置における印刷ジョブの処理状況に関するジョブ情報の構成例を表す図。

【図4】本発明の実施の形態に係る画像出力システムXにおける印刷ジョブの概略の伝送

50

経路を模式的に表した図。

【図 5】本発明の実施の形態に係る画像出力システム X における印刷ジョブの出力処理の手順を表すフローチャート。

【図 6】本発明の実施の形態に係る画像出力システム X を構成する P C の画面例を表す図。

【図 7】本発明の第 1 の実施例に係る画像出力システムにおける印刷ジョブの概略の伝送経路を模式的に表した図。

【図 8】本発明の第 1 の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャート。

【図 9】本発明の第 1 の実施例に係る画像出力システムにおける画像出力装置のハードディスクからの印刷ジョブの消去処理の手順を表すフローチャート。 10

【図 10】本発明の第 2 の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャート。

【図 11】本発明の第 3 の実施例に係る画像出力システムにおける印刷ジョブの出力処理の手順を表すフローチャート。

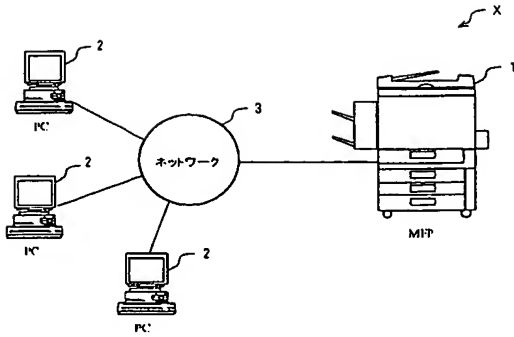
【符号の説明】

- 1 … 複合機能プリンタ（画像出力装置）
- 2 … パーソナルコンピュータ（情報処理装置）
- 3 … ネットワーク
- 1 1 … C P U
- 1 2 … ジョブ管理部
- 1 3 … ハードディスクドライブ（不揮発性メモリ，記憶手段）
- 1 4 … R A M（揮発性メモリ，記憶手段）
- 1 5 … F A X 機能部
- 1 6 … 暗号復号部（復号化手段，暗号化手段）
- 1 7 … 通信部
- 1 8 … プリントエンジン
- 1 9 … スキャナ
- 2 1 … C P U
- 2 2 … R A M
- 2 3 … R O M
- 2 4 … 操作部
- 2 5 … 表示部
- 2 6 … ハードディスクドライブ
- 2 7 … 通信部
- J D … ジョブ情報（画像処理状況に関する情報）
- P 1 … アプリケーションソフト
- P 2 … プリンタドライバ（画像データ送信プログラム）
- S 1 0 1, S 1 0 2, , … 処理手順（ステップ）

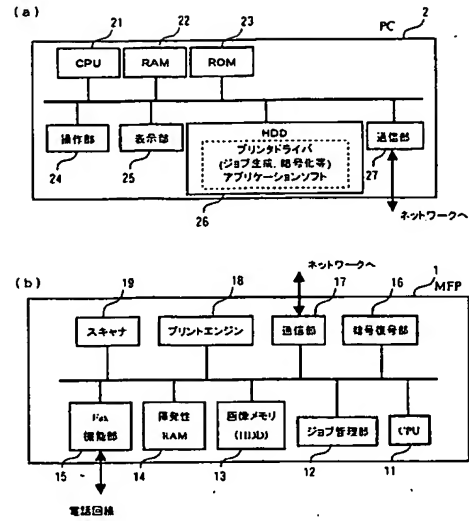
20

30

【図 1】



【図 2】



【図 3】

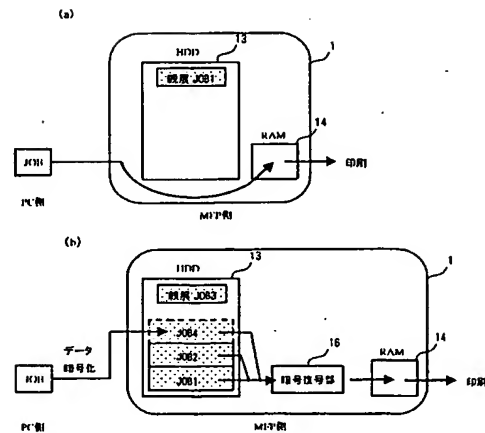
(a) ジョブ情報

JobNo.	ユーザ名	暗号化	状態	機能	属性	サイズ
1	Taiyo	あり	HDD保存	プリンタ	促進	122kB
2	Hanako	なし	受信中	プリンタ	待ち	121kB
.
.

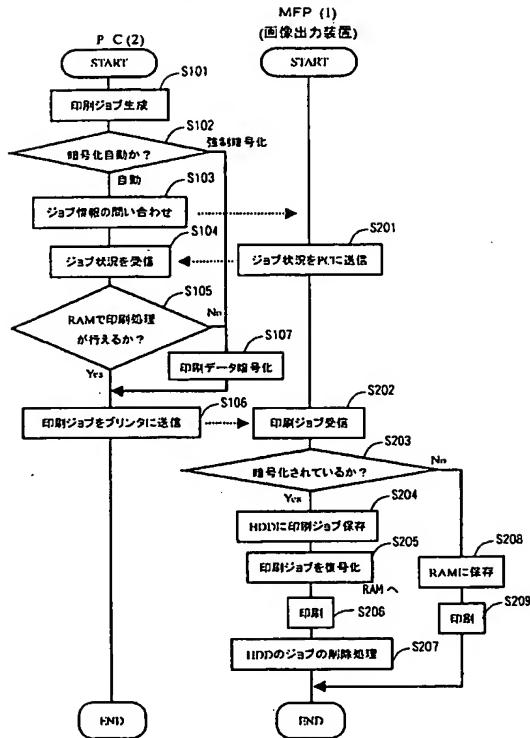
(b) ジョブ情報

JobNo.	ユーザ名	暗号化	状態	機能	属性	サイズ
1	Taro	なし	印字中	プリンタ	待ち	123kB
2	Suzuki	あり	HDD保存	コピー	待ち	119kB
3	Taiyo	あり	HDD保存	Fax	促進	122kB
4	Hanako	あり	受信中	プリンタ	待ち	121kB
.
.

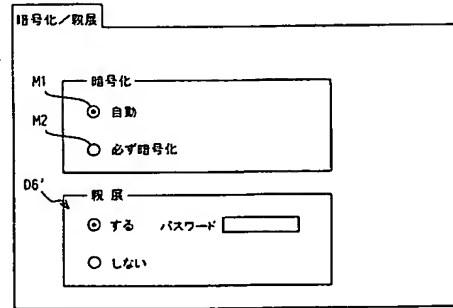
【図 4】



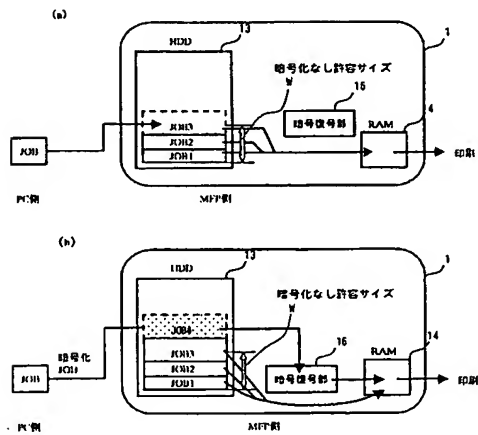
【図 5】



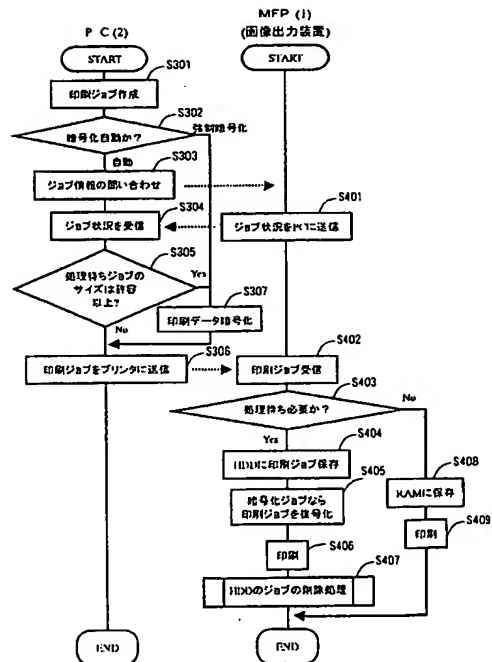
【図 6】



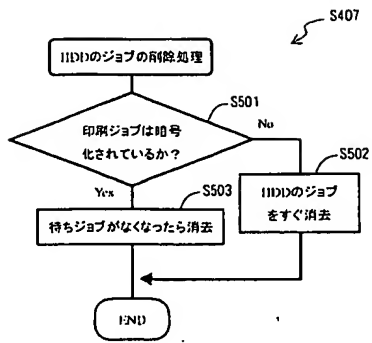
【図 7】



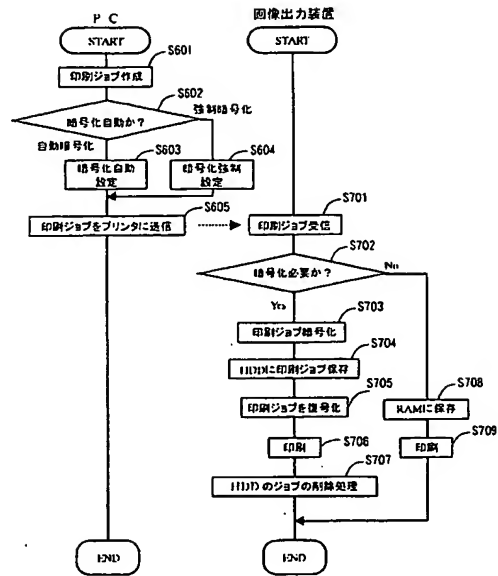
【図 8】



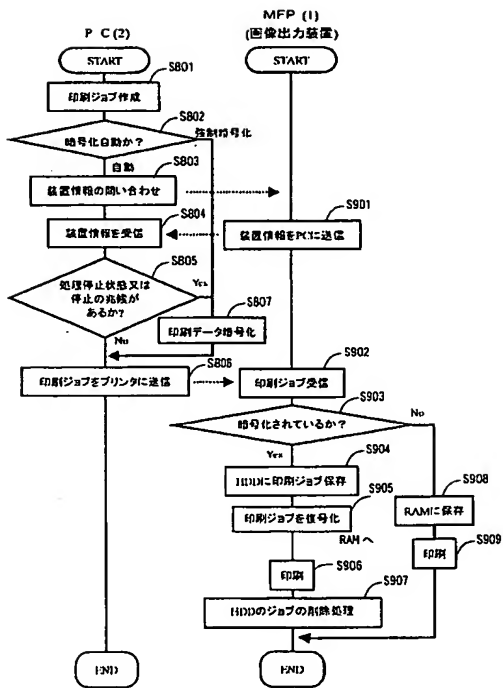
【図 9】



【図 10】



【図 11】



フロントページの続き

(51)Int.Cl.⁷

F I

テーマコード (参考)

H O 4 N 1/21

* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1]

In an image output system with which reception and memory to a memory measure are carried out for image data transmitted from an information processor by an image output device, and an output of said image data is made by this image output device,

An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation in said image output device,

An encoding means which enciphers said image data distinguished when it enciphered by said encryption discriminating means,

A decoding means which decrypts said image data provided and enciphered by said image output device before an output process,

An image data deleting means which eliminates image data which it was provided in said image output device, and an output process ended from said memory measure,

An image output system which possesses and is characterized by things.

[Claim 2]

Information about said image-processing situation includes information about an operating condition of volatile memory which constitutes said a part of memory measure,

The image output system according to claim 1 which is what will be distinguished if said encryption discriminating means enciphers about said image data which cannot be processed by use of said volatile memory within the limits among said memory measures in said image processing device.

[Claim 3]

Information about said image-processing situation includes information about quantity of image data of a processor limited, or its processing time,

Claim 1 which is what will be distinguished if said encryption discriminating means enciphers said image data when quantity of image data of said processor limited or its processing time is more than predetermined, or an image output system given in either of 2.

[Claim 4]

Information about said image-processing situation includes information about signs of a stop of image processing, and/or a stop of image processing,

The image output system according to any one of claims 1 to 3 which is what will be distinguished if said image data is enciphered when a possibility that said encryption discriminating means will be in a halt condition of image processing when said image output device is a halt condition of image processing is high.

[Claim 5]

The image output system according to claim 4 which is the information about 1 of the failures of information about a stop of said image processing of plugging of a recording form, a record slip of paper, a developer piece, and said image output device, or plurality.

[Claim 6]

The image output system according to claim 4 which is the information concerning [information about signs of a stop of said image processing] a residue of a recording form, and/or a residue of a developer.

[Claim 7]

The image output system according to any one of claims 1 to 6 which is that in which said image data deleting means eliminates promptly said image data which is not enciphered from said memory measure after the output process.

[Claim 8]

The image output system according to any one of claims 1 to 7 which is what is eliminated from said memory measure when said image data as which said image data deleting means is enciphered does not have image data of waiting for post-processing of the output process.

[Claim 9]

An image data transmitting means to which said image output device transmits information about said image-processing situation to said information processor is provided,

The image output system possessing an image data reception means in which said information processor receives information about said image-processing situation from said image output device, said encryption discriminating means, and said encoding means according to any one of claims 1 to 8.

[Claim 10]

The image output system according to any one of claims 1 to 8 with which said image output device possesses said encryption discriminating means and said encoding means.

[Claim 11]

Said image output device possesses said encryption discriminating means and an encryption discriminating information transmitting means which transmits discriminated result information on this encryption discriminating means to said information processor,

The image output system according to any one of claims 1 to 8 with which said information processor possesses an encryption discriminating information reception means which receives said encryption discriminating information from said image output device, and said encoding means.

[Claim 12]

In an image data transmission program which makes a computer perform processing which transmits image data used for a generating picture to an image output device,

Image data acquisition processing which acquires information about an image-processing situation from said image output device,

Encryption discrimination processing which distinguishes whether said image data is enciphered based on information about said image-processing situation,

Encryption processing which enciphers what was distinguished when it enciphered by said encryption discrimination processing among said image data transmitted to said image output device,

An image data transmission program performing a computer.

[Claim 13]

In an image data transmission program which makes a computer perform processing which transmits image data used for a generating picture to an image output device,

Encipherment information reception which receives information about whether said image data is enciphered from said image output device,

Encryption processing which enciphers image data transmitted to said image output device when information on a purport that it enciphers by said encipherment information reception is acquired,

An image data transmission program performing a computer.

[Claim 14]

In an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data,

An image data transmitting means which transmits information about an image-processing situation of said image data to said information processor,

A decoding means which decrypts said image data enciphered before an output process,

An image data deleting means which eliminates image data which an output process ended from said memory measure,

An image output device which possesses and is characterized by things.

[Claim 15]

In an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data,
An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation of said image data,
An encoding means which enciphers said image data distinguished when it enciphered by said encryption discriminating means,
A decoding means which decrypts said image data enciphered before an output process,
An image data deleting means which eliminates image data which an output process ended from said memory measure,
An image output device which possesses and is characterized by things.

[Claim 16]

In an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data,
An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation of said image data,
An encryption discriminating information transmitting means which transmits discriminated result information on said encryption discriminating means to said information processor,
A decoding means which decrypts said image data enciphered before an output process,
An image data deleting means which eliminates image data which an output process ended from said memory measure,
An image output device which possesses and is characterized by things.

[Claim 17]

The image output device according to any one of claims 14 to 16 which is that in which said image data deleting means eliminates promptly said image data which is not enciphered from said memory measure after the output process.

[Claim 18]

The image output device according to any one of claims 14 to 17 which is what is eliminated from said memory measure when said image data as which said image data deleting means is enciphered does not have image data of waiting for post-processing of the output process.

[Translation done.]

* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]

The image data transmitted from the information processor is received and memorized by an image output device, and this invention relates to the image data transmission program and image output device which are performed by the image output system with which the output of said image data is made by this image output device, and its information processor.

[0002]

[Description of the Prior Art]

By transmitting image data, such as print data constituted from information processors (henceforth a terminal), such as a personal computer, by image output devices, such as a printer, by image picture data, a Page Description Language, etc. via a network. Once the memory which an image output device possesses memorizes in the image output system which performs a generating picture (accumulation), it is common that a generating picture is carried out. In such an image output system, when unlawful access is made to the case where memories, such as a hard disk drive (HDD) of an image output device, are stolen, or an image output device, security reservation of the image data memorized by the memory poses a problem.

In order to solve such a problem conventionally, certainly enciphering the print job (an example of image data) memorized by HDD is shown in the patent documents 1.

[0003]

[Patent documents 1]

JP,2001-306273,A

[0004]

[Problem(s) to be Solved by the Invention]

However, if it is certainly enciphering image data, it is necessary to certainly perform decoding processing of image data before image output processing. For this reason, even if it was in an image-processing situation which does not have the image data of a processor limited and whose output process is possible immediately, for example, since decryption of image data was required, there was a problem that time until an output process is carried out became long.

Even if the image data memorized by the image output device was enciphered, when the memory state included the long time, the probability of receiving unlawful access and a theft became high, and the problem that security fell also had it. For example, when there are many the number and throughputs (the number of outputting parts, etc.) of image data (print job etc.) of a processor limited, processor-limited time until image processing (printing) is started becomes long. When image processing is in a halt condition with plugging (jam), a toner piece (developer piece), etc. of a recording form (paper), image processing cannot be performed until resumption of image processing is attained by release of jam, supply of a toner, etc. As a result, it becomes what image data (print job etc.) is memorized for by the image output device for a long time (it stagnates) (also in this case, the delivery date of fixtures, etc. think for several days by return), and is easy to lead to the fall of security.

Therefore, the place which this invention is made in light of the above-mentioned circumstances, and is made into the purpose, It is in providing the image data transmission program and image output device which are performed by the information processor which constitutes the image output system and it which can suppress processing time as much as possible, maintaining the security of the image data memorized by the image output device by which network connection was carried out.

[0005]

[Means for Solving the Problem]

To achieve the above objects, in an image output system with which reception and memory to a memory measure are carried out for image data to which this invention was transmitted from an information processor by an image output device, and an output of said image data is made by this image output device, An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation in said image output device, An encoding means which enciphers said image data distinguished when it enciphered by said encryption discriminating means, A decoding means which decrypts said image data provided and enciphered by said image output device before an output process, and an image data deleting means which eliminates image data which an output process ended from said memory measure are provided, and it is constituted as an image output system characterized by things.

Since it is determined by this whether encipher image-processing situation ***** image data,

when it is in an image-processing situation which can carry out the output process of the new image data comparatively for a short time, for example, Since probability of receiving unlawful access is low, processing according to a situation of carrying out an output process, without enciphering and shortening processing time is attained. As a result, it becomes possible to suppress processing time as much as possible, maintaining security of image data memorized by image output device.

Although eliminating only information (henceforth data management information) which manages access to the image data within memory measures, such as what is called FAT (FileAllocation Tables), itself as an elimination gestalt from said memory measure of image data here is also considered, In order to improve security nature more, it is desirable to eliminate by rewriting the image data itself to predetermined initialization data (henceforth full elimination).

[0006]

For example, information about said image-processing situation is a thing including information about an operating condition of volatile memory which constitutes said a part of memory measure. It is and what will be distinguished if said encryption discriminating means enciphers about said image data which cannot be processed by use of said volatile memory within the limits among said memory measures in said image processing device can be considered. when new image data can be processed by use of said volatile memory within the limits by image data of a processor limited not existing etc. according to such composition, an output process becomes quick, without enciphering a picture (namely, -- decryption is unnecessary). On the other hand, even when the theft of a main part of an image output device or its memory measure is carried out physically, since data in volatile memory which is not enciphered disappears while current supply stops, a leak of information is not produced. Generally, capacity of volatile memory is comparatively small, time when the same image data as volatile memory is accumulated since data in this memory is eliminated after processing is short, and it is hard to produce unlawful access which passes communication (network) between this short time. It becomes possible to save decryption time and to suppress processing time as much as possible, these results maintaining security of image data.

[0007]

Information about said image-processing situation is a thing including information about quantity of image data of a processor limited, or its processing time. It is and what will be distinguished if said encryption discriminating means enciphers said image data when quantity of image data of said processor limited or its processing time is more than predetermined is considered.

also by such composition, there is little quantity of image data of a processor limited, or when the processing time is less than predetermined, an output process becomes quick, without

enciphering image data (namely, -- decryption is unnecessary). Time until processing of image data is completed and is eliminated in this case is comparatively short simultaneously, and it is hard to produce unlawful access which passes communication (network) between this short time. It becomes possible to save decryption time and to suppress processing time as much as possible, these results maintaining security of image data.

[0008]

Information about said image-processing situation is a thing including information about signs of a stop of image processing, and/or a stop of image processing. It is and what will be distinguished if said image data is enciphered when a possibility that said encryption discriminating means will be in a halt condition of image processing when said image output device is a halt condition of image processing is high can be considered.

according to such composition, image processing is not a halt condition -- or when a possibility of being in a halt condition is low (there are no signs of a stop), an output process becomes quick, without enciphering image data (namely, -- decryption is unnecessary). Simultaneously, or processing of new image data is not started in this case, a possibility of being in a suspended state in the middle of processing is low, and a possibility of a processor limited or time of discontinuation of processing becoming long, and receiving a theft of memory storage and unlawful access is also low. As a result, it becomes possible to save decryption time and to suppress processing time as much as possible, maintaining security of image data.

Here, as information about a stop of said image processing, information about 1 of the failures of plugging of a recording form, a record slip of paper, a developer piece, and said image output device or plurality, etc. can be considered, for example.

As information about signs of a stop of said image processing, information about a residue of a recording form and/or a residue of a developer, etc. can be considered, for example.

[0009]

When there is no image data of waiting for post-processing of the output process, said image data which said image data which is not enciphered can consider what is promptly eliminated from said memory measure after the output process as said image data deleting means, and is enciphered on the other hand. What is eliminated from said memory measure can be considered.

Thereby, about low non-enciphering data of security nature, it is eliminated by the shortest storage time. About on the other hand comparatively safe data enciphered, since erasing processing is carried out when there is no processing load (there is no image data of a processor limited), speed of an output process is not affected. Since time is taken to perform this full elimination when performing said full elimination of image data especially, such processing is effective by prevention from influence to output speed.

[0010]

Here, the both-hands stage of said encryption discriminating means and said encoding means can consider a case where it provides in said case [where it provides in said information processor side], and image output device side, respectively.

(When providing said both-hands stage in an information processor)

For example, said image output device receives said information processor in information about said image-processing situation. What possesses an image data transmitting means which transmits and possesses an image data reception means in which said information processor receives information about said image-processing situation from said image output device, said encryption discriminating means, and said encoding means can be considered.

(When providing said both-hands stage in an image output device)

That in which said image output device possesses said encryption discriminating means and said encoding means is also considered.

(When distributing and providing said both-hands stage in an information processor and an image output device)

Said image output device receives said information processor in discriminated result information on said encryption discriminating means and this encryption discriminating means. An encryption discriminating information transmitting means which transmits is provided, and that in which said information processor possesses an encryption discriminating information reception means which receives said encryption discriminating information from said image output device, and said encoding means is also considered.

[0011]

This invention may be regarded as an image data transmission program executed by said information processor which constitutes said image output system. Composition changes with cases where a both-hands stage of said encryption discriminating means and said encoding means is provided in said case [where it provides in said information processor side, respectively], and image output device side also about this.

(When providing said both-hands stage in an information processor)

For example, in an image data transmission program which makes a computer perform processing which transmits image data used for a generating picture to an image output device, Image data acquisition processing which acquires information about an image-processing situation from said image output device, Encryption discrimination processing which distinguishes whether said image data is enciphered based on information about said image-processing situation, An image data transmission program making a computer perform encryption processing which enciphers what was distinguished when it enciphered by said encryption discrimination processing among said image data transmitted to said image output device can be considered.

[0012]

(When distributing and providing said both-hands stage in an information processor and an image output device)

Or in an image data transmission program which makes a computer perform processing which transmits image data used for a generating picture to an image output device, Encipherment information reception which receives information about whether said image data is enciphered from said image output device, When information on a purport that it enciphers by said encipherment information reception is acquired, an image data transmission program making a computer perform encryption processing which enciphers image data transmitted to said image output device is also considered.

[0013]

This invention may be regarded as said image output device which constitutes said image output system. Composition changes with cases where a both-hands stage of said encryption discriminating means and said encoding means is provided in said case [where it provides in said information processor side, respectively], and image output device side also about this.

(When providing said both-hands stage in an information processor)

For example, in an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data, An image data transmitting means which transmits information about an image-processing situation of said image data to said information processor, A decoding means which decrypts said image data enciphered before an output process, and an image data deleting means which eliminates image data which an output process ended from said memory measure are provided, and an image output device characterized by things can be considered.

[0014]

(When providing said both-hands stage in an image output device)

Or in an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data, An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation of said image data, An encoding means which enciphers said image data distinguished when it enciphered by said encryption discriminating means, A decoding means which decrypts said image data enciphered before an output process, and an image data deleting means which eliminates image data which an output process ended from said memory measure are provided, and an image output device characterized by things is also considered.

[0015]

(When distributing and providing said both-hands stage in an information processor and an image output device)

Or in an image output device which performs reception and memory to a memory measure for image data transmitted from an information processor, and outputs this image data, An encryption discriminating means which distinguishes whether said image data is enciphered based on information about an image-processing situation of said image data, An encryption discriminating information transmitting means which transmits discriminated result information on said encryption discriminating means to said information processor, A decoding means which decrypts said image data enciphered before an output process, and an image data deleting means which eliminates image data which an output process ended from said memory measure are provided, and an image output device characterized by things is also considered.

[0016]

Also in the above image output devices, as said image data deleting means, Said image data which is not enciphered can consider what is promptly eliminated from said memory measure after the output process, and on the other hand, said image data enciphered can consider what is eliminated from said memory measure, when there is no image data of waiting for post-processing of the output process.

[0017]

[Embodiment of the Invention]

Referring to an accompanying drawing below, an embodiment of the invention and an example are described, and an understanding of this invention is presented. The following embodiments and examples are examples which materialized this invention, and are not a thing of the character which limits the technical scope of this invention.

The block diagram showing the outline composition of PC (personal computer) and an image output device which constitutes the figure which expresses here the outline composition of the image output system X which requires drawing 1 for an embodiment of the invention, and the image output system X which requires drawing 2 for an embodiment of the invention, Drawing 3 the image output system X concerning an embodiment of the invention. The figure showing the example of composition of the job information about the processing situation of the print job in the image output device to constitute, The figure which expressed typically the transmission route of the outline of the print job in the image output system X which drawing 4 requires for an embodiment of the invention, the flow chart showing the procedure of the output process of the print job in the image output system X which drawing 5 requires for an embodiment of the invention, Drawing 6 the image output system X concerning an embodiment of the invention. The example of a screen of PC to constitute. The figure which expresses, the figure which expressed typically the transmission route of the outline of the print job in the image output system which drawing 7 requires for the 1st example of this invention, the flow chart showing the procedure of the output process of the print job in the image output system which drawing

8 requires for the 1st example of this invention, The flow chart and drawing 10 showing the procedure of the erasing processing of the print job from the hard disk of the image output device in the image output system which drawing 9 requires for the 1st example of this invention Operation of the 2nd of this invention. The flow chart showing the procedure of the output process of the print job in the image output system concerning an example and drawing 11 are the flow charts showing the procedure of the output process of the print job in the image output system concerning the 3rd example of this invention.

[0018]

First, the entire configuration of the image output system X applied to an embodiment of the invention using drawing 1 is explained.

This image output system X, for example via the predetermined networks 3, such as IEEE802.3 conformity, It is connected so that communication is possible, and two or more PC2 (personal computer) which are an example of the compound function printer 1 (MFT:Multi function Printer) and an information processor which is an example of an image output device are constituted.

this image output system X -- a print job -- said PC2 -- it is transmitted from each to said MFT1 via the network 3, and the picture corresponding to the print job is printed by the recording form by said MFT1 which received this (output).

[0019]

Drawing 2 is a block diagram showing the outline composition of said PC2 and said MFT1.

As shown in drawing 2, said PC2 by CPU21 which performs various operations, and this CPU21. By RAM22 by which the program executed is developed, and said CPU21. The hard disk drive 26 (HDD) the indicators 25, such as the final controlling elements 24, such as ROM23 and the keyboard with which programs, such as BIOS performed, are memorized, and a mouse, a liquid crystal panel, and CRT, various driver software and an application program, and various data are remembered to be, It is a common personal computer possessing the communications department 27 grade which performs the data communications through said network 3.

the word-processing software for generating document data, image data, etc. used as the source data of a print job in said HDD26, and illustrating -- with the various application software P1, such as software, and this application software P1. The created data is changed into the print job which can be interpreted by said MFT1, and the printer driver P2 (an example of an image data transmission program) for performing processing which transmits this print job to said MFT1 via said communications department 27, etc. are installed. As a print job, image data, such as GDI (Graphics Device Interface), the command structure data of the hexadecimal number which comprised PDL (Page Description Language: Page Description Language) etc., etc. can be considered. About the print job which comprised PDL etc., after

being changed into image data before printing in said MFT1, it is printed.

Here the feature of said printer driver P2, The job information acquisition processing which acquires the information (henceforth job information) about the processing situation (image-processing situation) of a print job from said MFT1, It is constituted so that execution of the encryption processing which enciphers the print job's which distinguishes whether a print job being enciphered based on the information acquired by this job information acquisition processing, and transmits to said MFT1 if needed is possible. The details are mentioned later. [0020]

By said MFT1 building in ROM the predetermined program was remembered to be, and executing the program. CPU11 which performs various control and the operation of MFT1 concerned, the job management department 12 which performs management processing of the processing situation of the print job which received from said PC2, the hard disk drive 13 (HDD) which is the nonvolatile memory which memorizes a print job (image data), From RAM14 which is the nonvolatile memory which stores a print job temporarily in the case of the output process, and a manuscript, about the print job which received from the picture read with the scanner 19 which reads a picture, and this scanner 19, or said PC2 with an inkjet method, a laser beam method, etc. Via the print engine 18 which performs the generating picture (image formation) to a recording form, and said network 3. Said PC2 and communication. The communications department 17 which carries out, When the print job which received from said PC2 is enciphered, a telephone line from the function which carries out FAX transmission of the code decoding part 16 which decrypts the print job before an output process, and the manuscript image data read with said scanner 19 through a telephone line, or other facsimile machines. F which has a function which leads, and outputs the image data which received to said print engine 18, or is stored in said HDD13. The AX function part 15 grade is provided. The image data which it is read with said scanner 19 and carries out a generating picture (that is, a manuscript picture is copied), and the image data received by said facsimile function part 15 are also one of the print jobs, and the processing situation is managed by said job management department 12.

Said communications department 17 in said MFT1 and said communications department 27 in said PC2, It has the function to perform the encryption and its decryption on communication (HTTPS-IPsec-PPTP, L2TP, etc.) so that a print job may not be easily monitored in the middle of communication with said network 3. Encryption according [the encryption and decryption on this communication] to said printer driver P2 and decryption by said code decoding part 16 are certainly performed independently. Even when "A print job is transmitted, without enciphering" is written hereafter, encryption and decryption on this communication shall be performed. [0021]

Drawing 3 expresses the example of composition of the job information JD about the

processing situation of the print job managed by said job management department 12 of said MFT1.

Discernment of the sending person (transmitting agency) of the print job by the additional information of the print job whenever a print job is inputted into said job management department 12 from said PC2 from reception or said scanner 19, or said facsimile function part 15, discernment of whether the print job is enciphered, The print job is a thing corresponding to which function. Identify discernment of whether to be, the attribute of the print job, the size of the print job, etc., assign the job number D1 to the arrival order of each print job, and each discriminated result as the user name D2, the encipherment information D3, the function data D5, the attribution information D6, and the size information D7. It relates with a predetermined memory measure and memorizes.

Said function data D5 here the printer function which outputs the print job which received from said PC2, the copy function which outputs the image data (print job) read with said scanner 19, and the image data (print job) which is at said facsimile function part 15, and was received. They are identification information, such as a Fax function to output.

Said attribution information D6 is a confidential job of specific addressing to a user about whether it is the usual print job ("waiting") which should be added to queuing of an output process, and the print job by specification of a password etc. from the user. It is the identification information of whether to be a print job which should be stored in said HDD13 without outputting until an output instruction occurs (** which is not added to queuing of an output process).

Said job management department 12 monitors the storing situation of the data in said HDD13 and said RAM14, and the operation situation of other apparatus continuously, and it confirms whether each print job is in what kind of state, the state D4 also relates it with said job number D1, and it memorizes them. Whether is the print job saved said HDD13 and is in the state of a processor limited For example, ("HDD preservation"), The state D4 of it being under reception by) "in printing" and said communications department 17 grade whether is it transmitted to said RAM14 and is under output with said print engine 18 ("under reception") is managed. [(] It is managed so that the job information JD including these information D1-D7 may always be maintained by said job management department 12 at the newest state. And the print job which the output process was completed and was eliminated from said RAM14 and said HDD13 is eliminated also from said job information JD, and said job number D1 is newly assigned according to the elimination. Here, elimination of said print job is eliminated by said full elimination.

[0022]

In this image output system X, by processing of said printer driver P2 of said PC2. Said state D4 of said job information JD is acquired from said MFT1, and when it is judged that the output

process of image data can be performed by memory use of said RAM14 of said MFT1 within the limits based on said state D4 where it was acquired (namely, ** which does not use said HDD13), It will be distinguished if a print job is not enciphered. on the other hand, if said HDD13 is not used [memory use of said RAM14 of said MFT1 within the limits], namely, -- when it is judged that the output process of image data cannot be performed, it will be distinguished if a print job is enciphered.

At this image output system X, a judgment whether an output process can be performed by memory use of said RAM14 within the limits is made on the following standards by processing of said printer driver P2 of said PC2.

Namely, when the print job which is "under printing" does not exist in said state D4 (an example of the information about the operating condition of said volatile memory) in said job information JD. It is judged that said RAM14 (volatile memory) of said MFT1 is intact, and can process by memory use of this RAM14 within the limits. On the other hand, when the print job which is "under printing" in said state D4 exists, said RAM14 of said MFT1 is in use, and it is judged that it cannot process by memory use of this RAM14 within the limits.

[0023]

Here, a judgment whether an output process can be performed by memory use of said RAM14 within the limits may be made on standards other than the above.

For example, in [including the information on the availability of said RAM14 (an example of the information about the operating condition of said volatile memory)] said PC2 side to said job information JD, It is possible to distinguish, if the availability of said RAM14 comes out enough compared with the data size of a print job and can perform an output process by memory use of said RAM14 within the limits in a certain case etc.

[0024]

Drawing 4 (a) expresses typically the transmission route of the outline of the print job which is not enciphered with an arrow. In drawing 4, the print job as which the print job shown by a shading frame was enciphered is expressed, and the print job shown by a white frame expresses the print job which is not enciphered.

If the print job which is not enciphered is transmitted from said PC2 side as shown in drawing 4 (a), the print job will be directly stored temporarily said RAM14, without being stored in said HDD13 by said MFT1 side, and the output process by said print engine 18 will be performed. On the other hand, drawing 4 (b) expresses the transmission route of the outline of the print job enciphered typically with an arrow. If the print job enciphered is transmitted from said PC2 side as shown in drawing 4 (b), When the print job is once stored in said HDD13 by said MFT1 side (the print job is added to queuing of an output process in that case) and the turn of processing comes, while being decrypted by said code decoding part 16, It stores temporarily said RAM14 and the output process by said print engine 18 is performed.

[0025]

Next, the procedure of the output process of a print job is explained using the flow chart shown in drawing 5. Hereafter, S101, S102, and -- express the number of procedure (step). In drawing 5, the processing by the side of said PC2 is controlled by processing (performing is said CPU21) of said printer driver P2, and the processing by the side of said MFT1 is controlled by said CPU11.

First, the application software P1, such as a word processor, is started at said PC2 side, and a print job will be generated by said printer driver P2 if start-of-printing operation of the data created from said final controlling element 24 is made (S101). (creation)

Next, an input request screen as shown in drawing 6 by the indicator 25 of said PC2 is displayed, and selection input processing whether a print job is enciphered with the automatic mode M1 ("automatic") or to carry out in the forcible encryption mode M2 ("it certainly enciphers") is made (S102). At this time, the input process of confidential information D6' which becomes the origin of said attribution information D6 in said job information JD is also made. In this input process, the input of the password in the case of considering it as selection and the confidential job of whether to make a print job into a confidential job is performed. This confidential information D6' is transmitted to said MFT1 as additional information of a print job.

[0026]

In S102, when said automatic mode M1 is chosen, a demand of said job information JD is transmitted from said communications department 27 to said MFT1 (S103 (inquiry of job information)). On the other hand, in said MFT1 side, said newest job information JD is replied through said communications department 17 according to the demand from said job management department 12 (S201 (a job situation is transmitted to PC)).

It is distinguished whether said job information JD replied in this way is received in said communications department 27 of said PC2 side (S104 (a job situation is received)), and the output process (printing job) of a print job can perform by memory use of said RAM14 by the side of said MFT1 within the limits (S105). This distinction (judgment) is performed on the basis of whether there are some which are "under printing" in said state D4 in said job information JD, as mentioned above.

When it could not perform by memory use of said RAM14 within the limits and is distinguished in S105, or when said compulsive encryption mode M2 is chosen in S102, After a print job is enciphered by said printer driver P2 (S107), the print job after this encryption is transmitted to said MFT1 through said communications department 27 (S106), and the processing by the side of said PC2 is completed.

In S105, when it could perform by memory use of said RAM14 within the limits and is distinguished, it is transmitted to said MFT1 through said communications department 27 as it is, without being enciphered (S106), and the processing by the side of said PC2 ends a print

job.

[0027]

On the other hand, the print job from said PC2 is received through said communications department 17 at said MFT1 side (S202), and it is distinguished whether the print job is enciphered (S203).

Here, when the print job which received is not enciphered, storing (preservation) of the print job is directly carried out to said RAM14 (S208), and after a printing job (output process) (S209) is made with said print engine 18, the processing by the side of said MFT1 ends it. At this time, the print job in said RAM14 is eliminated from the inside of said RAM14 with the end of an output process. Here, elimination of the print job from said RAM14 (volatile memory) eliminates only said data management information, such as FAT instead of said full elimination. Even when the theft of said MFT1 the very thing or said RAM14 is carried out physically as for this, it is because the data in said RAM14 disappears while current supply stops, so a leak of information is not produced, and is because it can shorten blanking time. Of course, when improving confidentiality more, said full elimination may be performed.

When the print job which received was enciphered in S203 and it is distinguished, The print job is once stored in said HDD13 (preservation), and is added to queuing of an output process (said state D3 of said job information JD is set to "HDD preservation" by S204 and said job management department 12).

And the print job stored in said HDD13, when the turn of the processing comes, it decrypts by said code decoding part 16 -- having (encryption is canceled) -- it stores temporarily said RAM14 (S205), and output (printing) processing by said print engine 18 is performed further (S206).

And after the print job which the output process ended is eliminated from said HDD13 (S207) (said full elimination), the processing by the side of said MFT1 ends it. Of course, since the print job stored in said HDD13 is enciphered, it may be made to eliminate only said data management information, such as FAT, without carrying out said full elimination. Then, processing time is shortened rather than performing said full elimination from said HDD13 of a print job.

[0028]

Since encryption / un-enciphering of a print job are changed according to the operating condition of said RAM14 by the side of said MFT1 (image output device) according to this image output system X as shown above, When an output process can be performed in said RAM14, it is not necessary to perform decoding processing and enciphered erasing processing of the original print job, and processing time can be suppressed short.

And since the time stored temporarily said RAM14 is a short time very much, it does not generate the data leakage by unlawful access easily, either. Said RAM14 which is nonvolatile

memory does not generate the data leakage by the theft of a memory, either, in order that a memory content may not remain, if current supply stops.

[0029]

[Example]

(The 1st example)

With said image output system X, what does not restrict it to this although it distinguishes whether a print job is enciphered by the ability of an output process to be performed by memory use of said RAM14 of said MFT1 within the limits, and is distinguished by other standards is considered. Here, the 1st example that distinguishes whether a print job is enciphered by whether the data size (quantity) of the print job of a processor limited is more than prescribed size is described.

Also in this 1st example, it shall be distinguished whether based on said state D4 where said state D4 of said job information JD was acquired and acquired from said MFT1 by processing of said printer driver P2 of said PC2, a print job is enciphered like said embodiment.

Since the total size of the print job of the processor limited in said MFT1 is less than the encryption-less predetermined allowable size W, drawing 7 (a) expresses typically an outline transmission route in case the print job which is not enciphered is transmitted with an arrow. In drawing 7, the print job as which the print job shown by a shading frame was enciphered is expressed, and the print job shown by a white frame expresses the print job which is not enciphered.

As shown in drawing 7 (a), even if the print job transmitted from said PC2 side is not enciphered, The print job is stored in said HDD13 by said MFT1 side (in that case, the print job is added to queuing of an output process), when the turn of processing comes, it stores temporarily said RAM14 and the output process by said print engine 18 is performed.

On the other hand, since the total size of the print job of the processor limited in said MFT1 is more than the encryption-less predetermined allowable size W, drawing 7 (b) expresses typically an outline transmission route in case the enciphered print job is transmitted with an arrow. If the print job enciphered is transmitted from said PC2 side as shown in drawing 7 (b), When the print job is once stored in said HDD13 by said MFT1 side (the print job is added to queuing of an output process in that case) and the turn of processing comes, while being decrypted by said code decoding part 16, It stores temporarily said RAM14 and the output process by said print engine 18 is performed.

[0030]

As "size of a print job", when the print job is constituted by the subject in the image data (bit data), it is possible here to use the data sizes (byte etc.) of the print job itself, but. When a print job is constituted by the Page Description Language (PDL:page description language), the substantial value (size) which carried out estimated calculation of the data size of an outputted

image from the contents of the print job is used. For example, it is adding the value of data size according to the print copies with reference to the designation command of the print copies set as a print job (multiplication) etc. The time when the data size of an outputted image is the same and which image formation takes but depending on the image content may differ. For this reason, transposing the time reduced property which is set as the print job constituted by PDL and which registers processing time beforehand for every command (memory), and carried out estimated calculation of that processing time from the contents of the print job to the size of a print job, and using it is also considered. Hereafter, the value which carried out estimated calculation as mentioned above shall also be contained in "size (sum total) of a print job."

[0031]

Next, the procedure of the output process of the print job in the 1st example is explained using the flow chart shown in drawing 8. In drawing 8, the processing by the side of said PC2 is controlled by processing (performing is said CPU21) of said printer driver P2, and the processing by the side of said MFT1 is controlled by said CPU11.

Since the processing of S301-S304 by the side of said PC2 in drawing 8 and the processing of S401 by the side of said MFT1 corresponding to this are the same as that of S101-S104, and S201 in said image output system X shown by drawing 5, explanation is omitted here.

If said job information JD is received by said communications department 27 from said MFT1 side at said PC2 side (S304), Based on this job information JD, it is distinguished whether the total size of the print job of the processor limited in said MFT1 is more than said encryption-less allowable size W (S305). Here, the total size of the print job of a processor limited is called for when said attribution information D6 in said job information JD totals said size information D7 about the print job which is "waiting."

In S302 when it is distinguished in S105 that the total size of the print job of a processor limited is more than said encryption-less allowable size W, When said compulsive encryption mode M2 is chosen, after a print job is enciphered by said printer driver P2 (S307), the print job after this encryption is transmitted to said MFT1 through said communications department 27 (S306), and the processing by the side of said PC2 is completed.

In S305, when it is distinguished that the total size of the print job of a processor limited is less than said encryption-less allowable size W, it is transmitted to said MFT1 through said communications department 27 as it is, without being enciphered (S306), and the processing by the side of said PC2 ends a print job.

[0032]

On the other hand, the print job from said PC2 is received through said communications department 17 at said MFT1 side (S402), and it is distinguished whether the print job needs to carry out a processor limited (S403). (that is, does the print job of "waiting" already exist in said

attribution information D6 or not?)

Here, when the necessity for a processor limited did not have the print job which received and it is distinguished, storing (preservation) of the print job is directly carried out to said RAM14 (S408), and after a printing job (output process) (S409) is made with said print engine 18, the processing by the side of said MFT1 ends it. At this time, the print job in said RAM14 is eliminated from the inside of said RAM14 with the end of an output process.

When the print job which received needed to be a processor limited in S403 and it is distinguished, The print job is once stored in said HDD13 (preservation), and is added to queuing of an output process (said state D3 of said job information JD is set to "HDD preservation" by S404 and said job management department 12).

And the print job stored in said HDD13, If checked and enciphered whether it is enciphered when the turn of the processing comes, after being decrypted by said code decoding part 16, if not enciphered, it is stored temporarily as it is said RAM14 (S405), Furthermore, output (printing) processing by said print engine 18 is performed (S406).

And after the print job which the output process ended is eliminated by the erasing processing of the print job from said HDD13 mentioned later (S407), the processing by the side of said MFT1 ends it.

[0033]

Drawing 9 is a flow chart showing the procedure of the erasing processing of the print job from said HDD13. This processing is controlled by said CPU11 of said MFT1.

It is distinguished whether the print job in said HDD13 in which the output process was able to be managed with this erasing processing is enciphered (S501), If not enciphered, when said full elimination is made (S502) and the print job is promptly enciphered from said HDD13, It waits until the print job of a processor limited is lost, and said full elimination is made from said (of course, when there is already no print job of a processor limited, it is promptly) HDD13. When the print job is enciphered, it may be made to eliminate only said data management information, such as FAT, here.

[0034]

Since encryption / un-enciphering of a print job are changed according to the size (quantity) of the print job of the waiting for the output process by the side of said MFT1 (image output device) according to the image output system concerning the 1st example as shown above, When the size of the print job of a processor limited is small, it is not necessary to perform decoding processing and processing time can be suppressed short.

And since the time to the completion of an output of the newly added print job and elimination just behind that is a short time comparatively if the size of the print job of a processor limited is small, it is hard to generate the data leakage by unlawful access.

On the other hand, since a print job is enciphered when the size (total size) of the print job of a

processor limited is large, it can prevent carrying out a data leakage by unlawful access etc. into a processor limited (fall of security).

The probability that the trouble to which it leads during processing of the print job of precedence that the size of the print job of a processor limited is large (processing time is long) to the stop of image processing, such as a toner piece, a record slip of paper, and jam, will occur also becomes high. Therefore, although the holding time of a print job (image data) becomes longer by generating of such a trouble and a possibility of receiving unlawful access and a theft becomes higher, since the print job is enciphered in this case, the fall of security is suppressed to the minimum.

About the enciphered comparatively safe print job, since it is deleted after the print job of a processor limited is lost, the blanking time from said HDD13 of a print job does not affect the processing time of other print jobs.

[0035]

(The 2nd example)

Although each of said embodiment and said 1st example performed distinction of whether to encipher a print job, and encryption of the print job by said PC2 side (information processor side), it may not be restricted to this and may be performed by said MFT1 side (image output device side).

Drawing 10 is a flow chart showing the procedure of the output process of the print job in the image output system concerning the 2nd example that performs distinction of whether to encipher a print job, and encryption of a print job by said MFT1.

First, the application software P1, such as a word processor, is started at said PC2 side, and a print job will be generated by said printer driver P2 if start-of-printing operation of the data created from said final controlling element 24 is made (S601). (creation)

Next, selection input processing whether it enciphers by the indicator 25 of said PC2 or to carry out in said compulsive encryption mode M2, and the input process of said confidential information D6' are made with said automatic mode M1 (S602 (refer to drawing 6)). Said confidential information D6' inputted here is transmitted to said MFT1 as additional information of a print job.

In S602, when said automatic mode M1 is chosen, the identification information of the purport that it is said automatic mode M1 is added to a print job (S604), When said compulsive encryption mode M2 is chosen, the identification information of the purport that it is in said compulsive encryption mode M2 is added to a print job (S603).

And it is transmitted to said MFT1 side through said communications department 27, without enciphering a print job as it is with said identification information (S605), and the processing by the side of said PC2 is completed.

[0036]

On the other hand, the print job from said PC2 is received through said communications department 17 at said MFT1 side (S701), and the necessity of encryption of the print job is distinguished (S702).

Here, when the information on the purport that a print job is in said compulsive encryption mode M2 is added, it is distinguished irrespective of the contents of said job information JD that encryption is required.

When the information on the purport that it is said automatic mode M1 is added, it is distinguished in accordance with the distinction standard of S105 in drawing 5 mentioned above based on said job information JD whether a print job is enciphered (necessity).

In S702, when encryption of a print job is distinguished as it is unnecessary, storing (preservation) of the print job is directly carried out to said RAM14 (S708), and after a printing job (output process) (S709) is made with said print engine 18, the processing by the side of said MFT1 ends it. At this time, the print job in said RAM14 is eliminated from the inside of said RAM14 with the end of an output process.

In S702, when encryption of the print job which received is distinguished as it is required, the print job is enciphered by said code decoding part 16 (S703), and the enciphered print job is stored in said HDD13 (S704). (preservation) At this time, that print job is added to queuing of an output process (said state D3 of said job information JD is set to "HDD preservation" by said job management department 12). In addition to an enciphering function, said code decoding part 16 shall also have a decoding function.

And the print job stored in said HDD13, when the turn of the processing comes, it decrypts by said code decoding part 16 -- having (encryption is canceled) -- it stores temporarily said RAM14 (S705), and output (printing) processing by said print engine 18 is performed further (S706).

Next, after said full elimination (S707) is made from said HDD13, the processing by the side of said MFT1 ends the print job which the output process ended. Of course, since the print job stored in said HDD13 is enciphered, it may be made to eliminate only said data management information, such as FAT, without carrying out said full elimination.

Since encryption is performed by MFT1 side according to the composition of this 2nd example, It is more effective on security at the point which can encipher like [which are transmitted from said PC2 / not only a print job but a job of a copy, a job of FAX, etc.] the print job from said PC2 side.

[0037]

Even distinction of whether to encipher by said MFT1 side may be performed, and the discriminated result may be transmitted to said PC2, and according to said discriminated result received to said PC2 side which received this, it may constitute so that a print job may be enciphered, only when required.

For example, it transposes to the processing which requires the encryption discriminating information about whether S103 of drawing 5 is enciphered to said PC2 to said MFT1. After the discrimination processing (for example, processing of drawing 10 of S702) of whether to encipher, it constitutes from said MFT1 side which received this demand so that it may reply to said PC2 by making that discriminated result into said encryption identification information from said MFT1 instead of S201 of drawing 5.

The discrimination processing of S105 by the side of said PC2 is constituted so that whether it is enciphering (S107) may change according to said encryption identification information.

Embodying this invention by such composition is also considered.

[0038]

(The 3rd example)

Whether said embodiment and said 1st example encipher a print job by the ability of an output process to be performed by memory use of said RAM14 of said MFT1 within the limits. It distinguishes, or although distinguished by whether the data size (quantity) of the print job of a processor limited is more than prescribed size, what is not restricted to this and distinguished by other standards is considered. here, the 3rd example distinguished on the basis of the information about the stop of image processing or its signs is started [whether a print job is enciphered and] -- image output system ***** explanation is given.

Drawing 11 is a flow chart showing the procedure of the output process of the print job in the image output system concerning the 3rd example of this invention.

S101-S106 of drawing 5 which S801-S806 which are shown in drawing 11 mentioned above The processing of S801-S806 by the side of said PC2 in drawing 11 and the processing of S901-S909 by the side of said MFT1 corresponding to this are equivalent to the processing of S101-S106, and S201-S209 in said image output system X shown by drawing 5. A point which is different here by the processing shown in drawing 11, and the processing shown in drawing 5, The processing of S805 by the side of the point that the information transmitted and received by S901 and S804 is said not job information JD but information (henceforth device information) about the stop of image processing in said MFT1 or its signs, and said PC2 based on said device information a print job. It is a point which is the processing which distinguishes whether it enciphers or not, and other processings are the same as the processing shown in drawing 5.

[0039]

Jam [in / in said device information / said MFT1] (plugging of a recording form), a record slip of paper (paper piece), a toner piece (developer piece), and the information (an example of the information about the stop of said image processing) about failure of said MFT1, The information (an example of the information about the signs of a stop of image processing) about the residue (the number of ** sheets) of a recording form and the residue of a toner

(developer) is included.

And when are generated by jam, being generated by the record slip of paper in S805 by the side of said PC2 and being generated by the toner piece, and when failure has occurred in said MFT1 and the residue (the number of ** sheets) of a recording form is less than a specified number further. Or when toner residue is less than the specified quantity, After a print job is enciphered by said printer driver P2 (S807), in being other, it is transmitted to said MFT1 through said communications department 27, without being enciphered (S806), and the processing by the side of said PC2 ends a print job.

Thereby, image processing cannot be performed until resumption of image processing is attained by release of jam, supply of a recording form and a toner, etc.

By this, with jam, a toner piece, etc., since there are little case where image processing is not a halt condition, recording form residue, and toner residue. When a possibility that processing will be in a halt condition on the way is low (there are no signs of a stop), since a print job (image data) is not enciphered, the output process of a picture becomes quick (namely, since there is no necessity for decryption). Simultaneously, or processing of a print job is not started, a possibility of being in a suspended state in the middle of processing is low, and a possibility of receiving unlawful access which a processor limited or the time of discontinuation of processing became long, and led the theft and network of said image memory 13 is also low. As a result, it becomes possible to save decryption time and to suppress processing time as much as possible, maintaining the security of a print job.

By the procedure as what was shown in drawing 10 in which it is the same also when distinguishing whether a print job is enciphered in this way on the basis of the information about the stop of image processing, or its signs. It is possible to constitute so that distinction of whether to encipher a print job and encryption of a print job may be performed by said MFT1. In this case, what is necessary is just to perform the same discrimination processing as S805 of drawing 11 in the discrimination processing of S702 of drawing 10.

[0040]

[Effect of the Invention]

As explained above, according to this invention, since it is determined whether encipher image-processing situation ***** image data, it becomes possible to suppress processing time as much as possible, maintaining the security of the image data memorized by the image output device.

[Brief Description of the Drawings]

[Drawing 1]The figure showing the outline composition of the image output system X concerning an embodiment of the invention.

[Drawing 2]The block diagram showing the outline composition of PC (personal computer) and an image output device which constitutes the image output system X concerning an

embodiment of the invention.

[Drawing 3]The figure showing the example of composition of the job information about the processing situation of the print job in the image output device which constitutes the image output system X concerning *****.

[Drawing 4]The figure which expressed typically the transmission route of the outline of the print job in the image output system X concerning an embodiment of the invention.

[Drawing 5]The flow chart showing the procedure of the output process of the print job in the image output system X concerning an embodiment of the invention.

[Drawing 6]The figure showing the example of a screen of PC which constitutes the image output system X concerning an embodiment of the invention.

[Drawing 7]The figure which expressed typically the transmission route of the outline of the print job in the image output system concerning the 1st example of this invention.

[Drawing 8]The flow chart showing the procedure of the output process of the print job in the image output system concerning the 1st example of this invention.

[Drawing 9]The flow chart showing the procedure of the erasing processing of the print job from the hard disk of the image output device in the image output system concerning the 1st example of this invention.

[Drawing 10]The flow chart showing the procedure of the output process of the print job in the image output system concerning the 2nd example of this invention.

[Drawing 11]The flow chart showing the procedure of the output process of the print job in the image output system concerning the 3rd example of this invention.

[Description of Notations]

1 -- Compound function printer (image output device)

2 -- Personal computer (information processor)

3 -- Network

11 -- CPU

12 -- Job management department

13 -- Hard disk drive (nonvolatile memory, memory measure)

14 -- RAM (volatile memory, memory measure)

15 -- Facsimile function part

16 -- Code decoding part (a decoding means, encoding means)

17 -- Communications department

18 -- Print engine

19 -- Scanner

21 -- CPU

22 -- RAM

23 -- ROM

24 -- Final controlling element

25 -- Indicator

26 -- Hard disk drive

27 -- Communications department

JD -- Job information (information about an image-processing situation)

P1 -- Application software

P2 -- Printer driver (image data transmission program)

S101, S102, -- procedure (step)

[Translation done.]

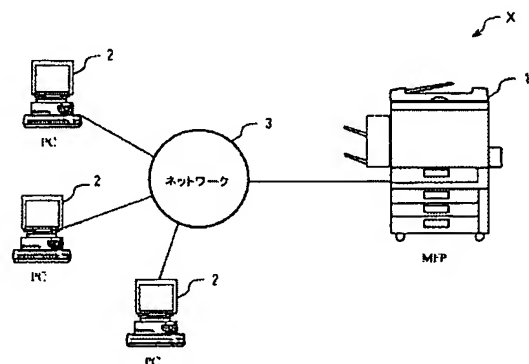
* NOTICES *

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

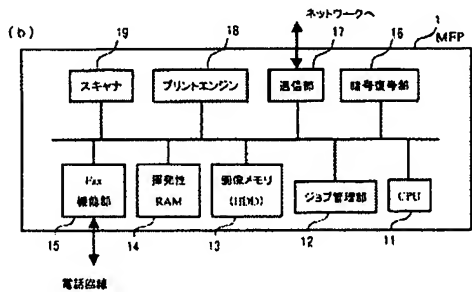
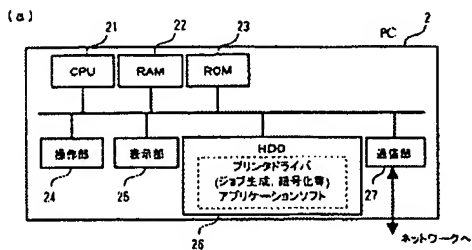
- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.*** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DRAWINGS

[Drawing 1]



[Drawing 2]



[Drawing 3]

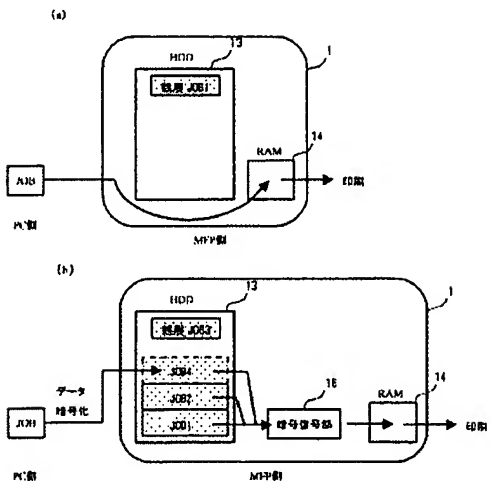
(a) ジョブ情報

JobNo.	ユーザ名	暗号化	状態	機能	属性	サイズ
1	Taiyo	あり	HDD 保存	プリンタ	複製	128kb
2	Haseko	なし	受信中	プリンタ	待ち	121kb
.						
.						

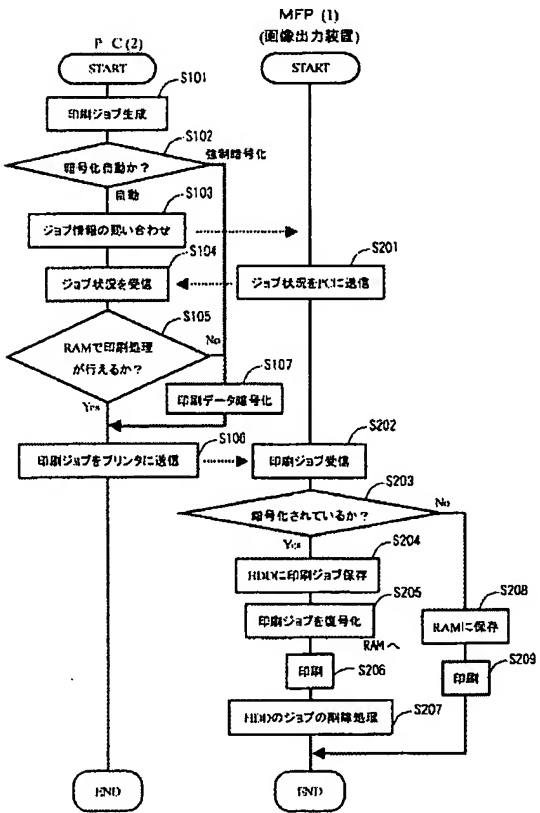
(b) ジョブ情報

JobNo.	ユーザ名	暗号化	状態	機能	属性	サイズ
1	Iano	なし	印字中	プリンタ	待ち	123kb
2	Suzuki	あり	HDD 保存	コピー	待ち	111kb
3	Taiyo	あり	HDD 保存	Fax	複製	122kb
4	Haseko	あり	受信中	プリンタ	待ち	121kb
.						
.						

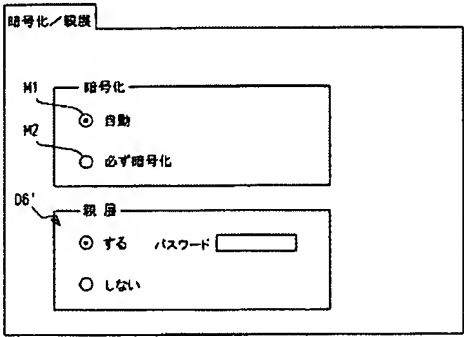
[Drawing 4]



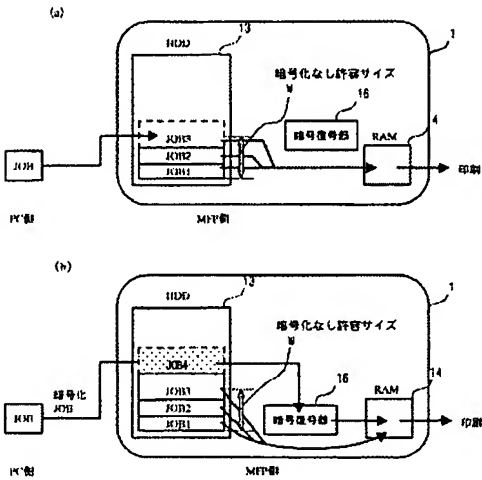
[Drawing 5]



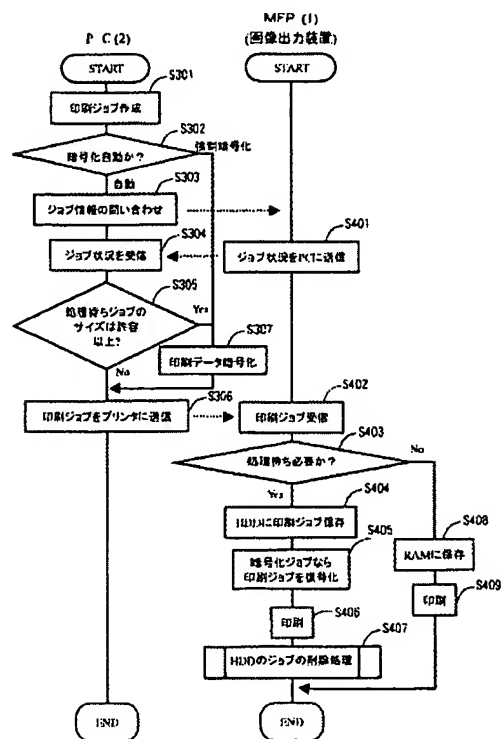
[Drawing 6]



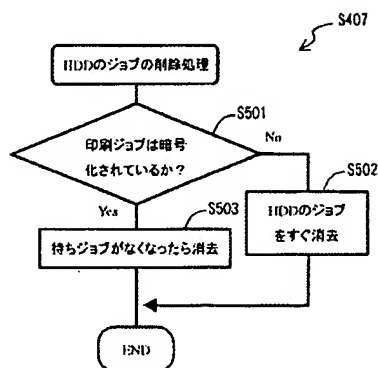
[Drawing 7]



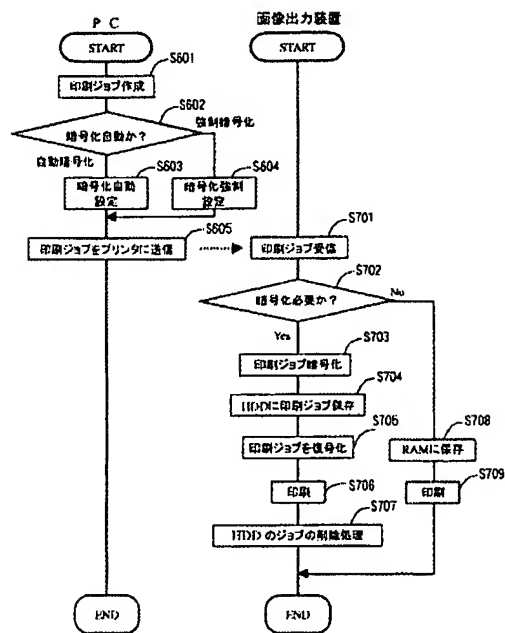
[Drawing 8]



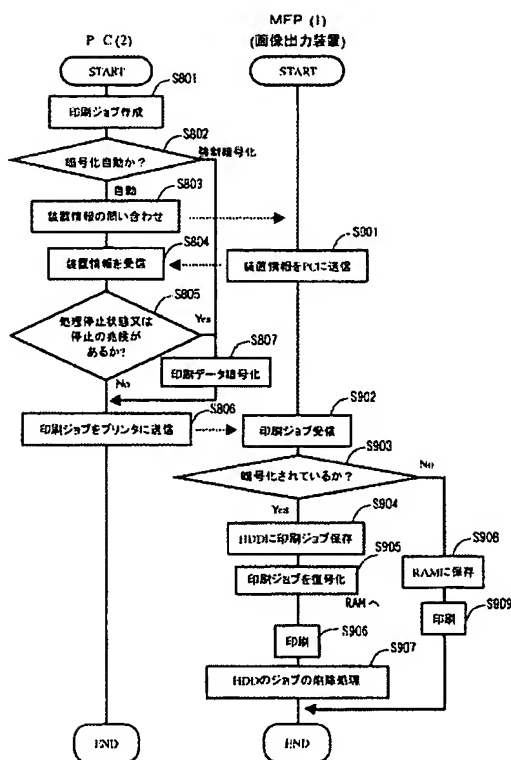
[Drawing 9]



[Drawing 10]



[Drawing 11]



[Translation done.]